

4

LESSON

Managing Applications, Services, Folders, and Libraries

EXAM OBJECTIVE MATRIX

SKILLS/CONCEPTS	EXAM OBJECTIVE DESCRIPTION	EXAM OBJECTIVE NUMBER
Installing and Managing Applications	Understand application installations.	3.1
Understanding Services	Understand services.	3.4
Using MSCONFIG (System Configuration utility)	Understand native applications and tools.	1.3
Understanding File Systems	Understand file systems.	4.1
Exploring and Managing Libraries	Understand libraries.	4.4
Encrypting and Compressing Files and Folders	Understand encryption. Understand storage.	4.3 5.2

KEY TERMS

Active Directory

application

assign

BitLocker Drive Encryption

compression

EFS certificate

Encrypting File System (EFS)

encryption

encryption key

FAT

FAT32

file system

Group Policy

Group Policy object (GPO)

install application

library

local application

MSCONFIG

multi-booting

NTFS

Programs and Features

publish

services

System Configuration utility

uninstall application

At Interstate Snacks, Inc., management wants to maximize the return on their investment in Windows 7. The IT group has requested that you prepare user training materials to teach employees how to make best use of Windows 7 files, applications, libraries, and file encryption. You need to learn as much as possible about these technologies to provide accurate materials and in-depth training.

■ Installing and Managing Applications



THE BOTTOM LINE

You **install applications**, or programs, either at the local level or the network level. A local installation results in the software files running directly from a computer. Installing over a network generally means the software files are made available from an application server on a network. The network method, along with Group Policy, gives an administrator more efficient control over who can use the software and who can remove it.

TAKE NOTE *

The terms “application” and “program” are used interchangeably in this book.

CERTIFICATION READY

What are the differences between local and networked applications?
3.1

X REF

In Lesson 2, you learned about Microsoft Application Virtualization (App-V), which represents one way to deliver applications over a network. However, it requires a supporting virtualization infrastructure.

An **application** is a program that runs “on top” of the operating system or from a server, and helps a user perform a specific task, such as word processing, appointment scheduling, or accounting. Some applications are included with Windows—such as Notepad for simple text editing or Internet Explorer for browsing the Web. Other applications must be licensed from a software publisher, such as Microsoft, Adobe, and Intuit, and then installed on your computer locally or on a server.

This section explores application installation and management in Windows 7. Installing a single application on one computer is easy, although the installation process varies a bit depending on the application. Installing applications on many Windows 7 computers is more efficiently tackled using a network. For example, you can use Group Policy to install and control access to applications. **Uninstalling applications** is a breeze, whether local or over a network.

In Windows 7, users might access applications in a variety of ways. For applications that users must be able to run with or without network or Internet access, you should install those applications directly on individual computers. This involves running setup.exe or a Microsoft Installer (which usually has an .msi file extension) in Windows 7, or building a custom installation image that includes one or more pre-installed applications. In this case, you install the application directly onto a computer running Windows 7; it’s considered to be a **local application** because it stays with that computer.

If you’re working in a networked environment with a domain, it’s more efficient to store the application’s installation files in a network location; they are installed on the client computer or are available to run from the server when users log on. Many IT administrators want to maintain tight control over specific applications, so administrators require that all users access applications from a network rather than locally. As you’ll learn in this lesson, Group Policy gives administrators control over which users, computers, or groups can have access to applications.



INSTALL AN APPLICATION LOCALLY

GET READY. To install an application in Windows 7, perform the following steps:

1. Start the application’s installation program.
 - If installing from a CD/DVD, insert the application’s installation media into your computer’s CD/DVD drive. The installer program should run automatically.

- If installing an application you downloaded from the Web, or if the installer program doesn't start automatically when inserting a CD/DVD, open Windows Explorer, browse to the location of the application's installer program (such as **setup.exe**), and then double-click it.

2. Follow the prompts to install the application.

Every program is different, but most programs prompt you to accept the license agreement, select a location on your computer in which to install the software files, and then enter a product ID or key.

Removing or Uninstalling an Application

A user or administrator might need to remove, or uninstall, a local application for a variety of reasons. Windows 7 provides the Programs and Features applet in Control Panel for this purpose.

CERTIFICATION READY
How are applications removed or uninstalled?
3.1

Figure 4-1
Some applications provide uninstall utilities to remove the application from your computer

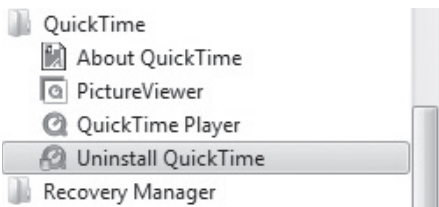
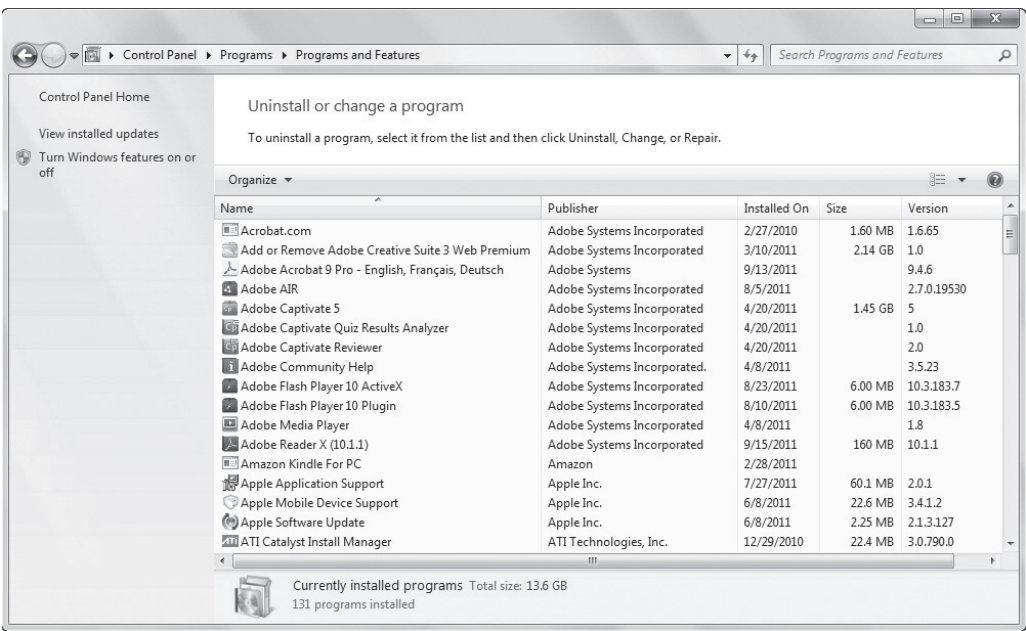


Figure 4-2
The Programs and Features applet in Control Panel



Using *Programs and Features*, simply browse the list of programs, click the program you want to uninstall, and then click Uninstall on the toolbar. Follow the prompts that display until the program is removed. You might be prompted to restart your computer.

X_{REF}

You'll learn about the Windows registry later in this lesson and in Lesson 7. You'll learn about Safe Mode, other boot options, and System Restore in Lesson 8.

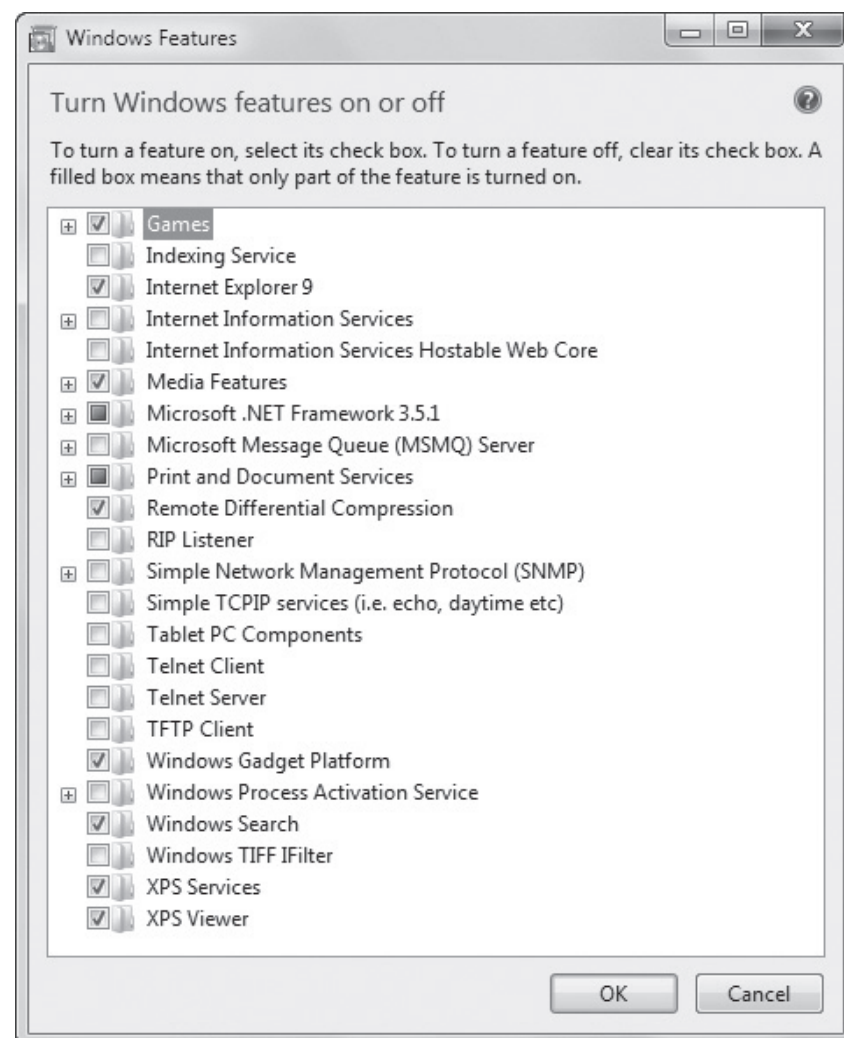
If the program does not uninstall properly, try running the uninstall process again. You can also try uninstalling the program in Safe Mode. Rolling back (or returning) to a previous system state using System Restore might also resolve the problem. Doing so, however, will also “uninstall” other programs that were installed since the last system restore point was saved. As a last resort, contact the software publisher to find out how to manually remove the application from your computer. (A manual removal involves editing the registry and deleting files and folders.)

Sometimes you simply need to change or repair a program rather than uninstall it. Some programs provide those options, which will display on the Programs and Features toolbar when you select the program in the list.

In addition, you can turn Windows features on and off—no installation/uninstall is required. In the Programs and Features window, in the left pane, click *Turn Windows features on or off*. In the Windows Features dialog box (see Figure 4-3), select the check boxes of features you want to turn on and deselect those you want to turn off.

Figure 4-3

The Windows Features dialog box



+ MORE INFORMATION

For more information about installing and uninstalling applications in Windows 7, visit <http://windows.microsoft.com/en-US/windows7/Install-a-program> and <http://windows.microsoft.com/en-US/windows7/Uninstall-or-change-a-program>, respectively.

Understanding Group Policy and Network Application Installation

In a Windows network in a domain environment, administrators can use Group Policy to ease the burden of administering and managing many users and client computers. Group Policy lets you control who may install software, and on which computers, and helps you push software updates and security configurations across the network. Group policies also exist in Windows 7 and other Windows operating systems. They are referred to as Local Group Policies and affect only the users who log on to a particular computer. This section focuses on Group Policy at the network domain level.

CERTIFICATION READY

How are network applications installed using Group Policy?

3.1

Group Policy is a collection of settings (policies) stored in Active Directory on a Windows network. **Active Directory** is an infrastructure (directory) that stores information and objects. An object can be a file, a printer, a computer, a user account, or other entities. Objects in Active Directory are linked to **Group Policy objects (GPOs)**, which are used by administrators to control users and computers on a network and to deploy applications, software updates, and security. Group Policy affects users and computers contained in sites, domains, and organizational units.

TAKE NOTE *

Group Policy is supported in Windows 7 Professional, Ultimate, and Enterprise editions. Active Directory was renamed Active Directory Domain Services in Windows Server 2008.

Group Policy works well in small to large environments whether an organization is located in a single area or has multiple offices spread around a state or several states, for example. It's easiest to manage in mostly "heterogeneous environments," in which many of the client computers use the same hardware and users use much of the same software with the same configurations.

If your organization has already deployed Active Directory, such as Microsoft Windows 2008 R2 Active Directory Domain Services (AD DS), using Group Policy to push applications to users or computers is efficient. Using Group Policy, you can **assign** or **publish** an application to all users or computers in a designated site, domain, organizational unit (OU), or to a local, individual user or computer.

For example, let's say you're deploying Microsoft Office for more than 20 users. If you set up Group Policy to assign the software on each *computer*, the software is installed the next time the computer starts and any users with the correct permissions who log on to the computer run the software. If you use Group Policy to assign the software to *users*, the next time an authorized user clicks the Microsoft Office shortcut or menu item, the software installs on the user's computer and Office opens. If you publish an application to users, the next time a user logs on, he can choose to install the software from a dialog box that appears.

With Group Policy, you can control which users can use the software. If a user logs on who isn't authorized to run the software (considered "out of scope"), the software can be uninstalled automatically.

Once software is installed, you can push updates to the software and even upgrade programs using Group Policy.



INSTALL AN APPLICATION FROM A NETWORK LOCATION

GET READY. Configuring Group Policy in Windows Server is beyond the scope of this book, but this exercise shows you how to install an application from a network location in a domain, from the user's perspective. Perform the following steps:

1. Click **Start > Control Panel > Programs > Programs and Features**. In the left pane, click **Install a program from the network**.

TAKE NOTE *

These steps work if you set the GPO to install an application to a *user* versus a *computer*.

2. Browse the list of programs, click a program you want to install, and then click **Install**.

Follow the prompts to move through the installation. You might be prompted for an administrator password or confirmation during the installation.

+ MORE INFORMATION

For more information about Group Policy in Windows 7, visit <http://windows.microsoft.com/en-US/windows7/Group-Policy-management-for-IT-pros>. To learn how to use Group Policy to remotely install software in Windows Server 2003 and in Windows Server 2008, visit <http://support.microsoft.com/kb/816102>

■ Understanding Services

**THE BOTTOM LINE**

Services run in the background on a Windows system to help the operating system run other programs. The Services console is the central management point of services in Windows Vista and Windows 7.

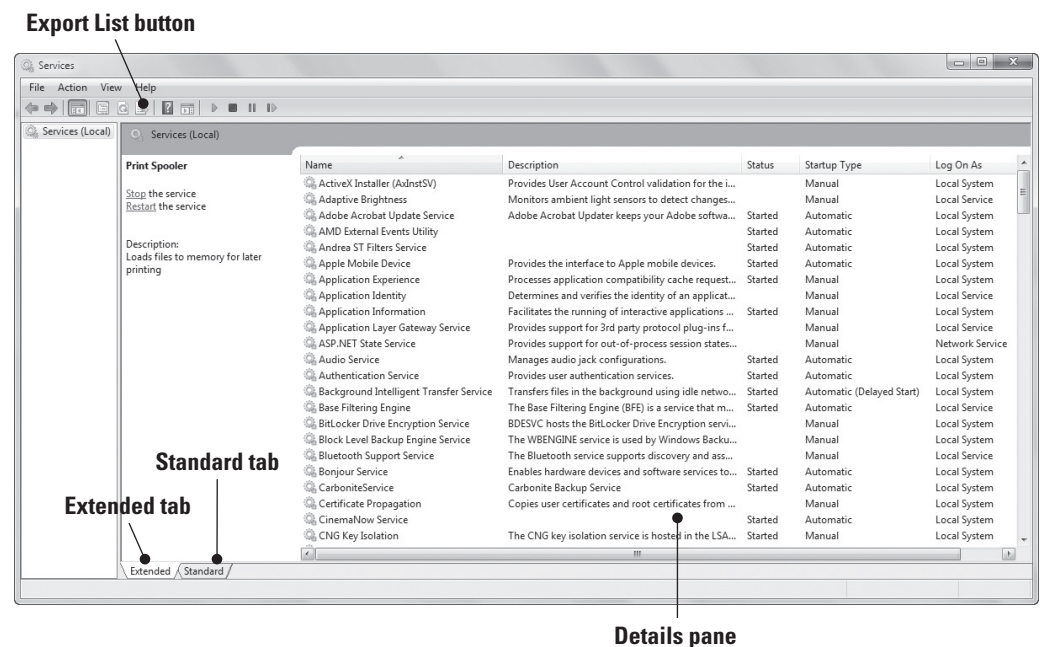
X REF

You learned about the MMC in Lesson 3.

Windows uses services to handle requests for print spooling, file indexing, task scheduling, the Windows Firewall, and much more. Services run in the background, essentially helping the operating system work with other programs. Although services do not usually have user interfaces, you can manage services through the Microsoft Management Console (MMC) Services snap-in (see Figure 4-4).

Figure 4-4

The Services console in Windows 7



A Windows 7 system can have more than 100 services running at any one time. Each computer can have different services running, depending on the version of Windows in use, the computer

manufacturer, and the applications installed, but Windows 7 generally uses many of the same services across its editions.

To use the Services snap-in and configure services, you must be a member of the Account Operators group, the Domain Admins group, or the Enterprise Admins group, or you must have received the appropriate authority. Using the **Run as** command to open the Services console ensures you have the proper level of authority.

You can access Windows services in many different ways:

- Click Start, type **services** in the *Search programs and files* search box, and then click Services or services.msc in the resulting list. (Or right-click Services or services.msc and select *Run as administrator*. You must provide an administrative password or confirm to continue.) The Services console displays.
- In Computer Management, expand the Services and Applications node and click Services.
- In Administrative Tools, double-click Services or double-click Component Services and then click Services.
- Open Task Manager and click the Services tab.
- Open MSCONFIG and click the Services tab. (MSCONFIG is covered in the next section in this lesson.)

The Extended and Standard tabs (at the bottom of the Services console) both display all of the services in the system; however, the Extended tab provides descriptive information for a selected service in the space to the left of the details pane. Sometimes a link is displayed for you to get more information about a particular service.

The Services console enables you to view all services and their status; add, start, stop, or disable services; select user accounts that might run the service (for security purposes); define how a service recovers from failures; or view a list of service, program, and driver dependencies. To use any of these options, double-click the service to open its Properties dialog box.

TAKE NOTE *

You can export service information to a .txt or .csv file.

CERTIFICATION READY

What are the four service startup types?

3.4

Understanding Service Startup Types

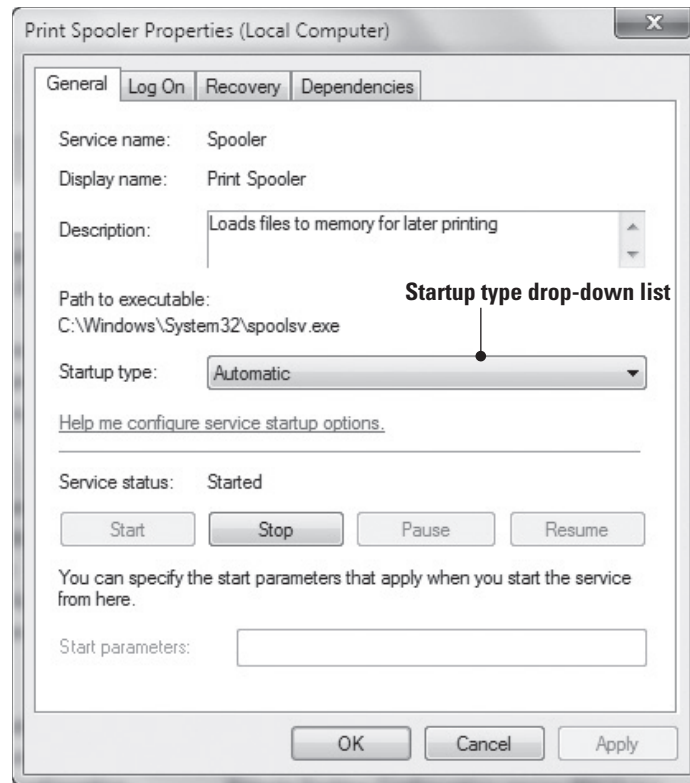
The General tab in the service's Properties dialog box (see Figure 4-5) provides options for setting a service's startup type:

- **Automatic (Delayed Start):** The service starts approximately two minutes after the operating system is up and running.
- **Automatic:** The service starts as the operating system starts.
- **Manual:** The service must be started manually, by a user, a dependent service, or a program.
- **Disabled:** The service is disabled and will not start.

TAKE NOTE *

Be careful when disabling any services. Some services, such as Security Center and Windows Firewall, should not be disabled unless the computer is behind a hardware firewall. Many computer users disable unnecessary services to optimize the speed of their computers. You should create a system restore point (covered in Lesson 8) before disabling services. And although it's time consuming, you should disable one service at a time, reboot your computer, and check for side effects of disabling that service before disabling any other services.

Figure 4-5
The General tab



You can also start, stop, pause, or resume a service using the buttons in the Service status section. For example, let's say a printer has several duplicate (unnecessary) print jobs and the queue is not responding. You've restarted the printer a few times but that didn't work. To fix the problem, just restart the Print Spooler service in the Services console to clear the print queues.

TAKE NOTE *

While troubleshooting a service, try pausing the service (if it's an option) and then unpausing the service before stopping and restarting the service. By pausing and then continuing, you might be able to resolve the problem without having to reset connections or cancel jobs.

CERTIFICATION READY

Which service or user accounts can you specify a service to use?

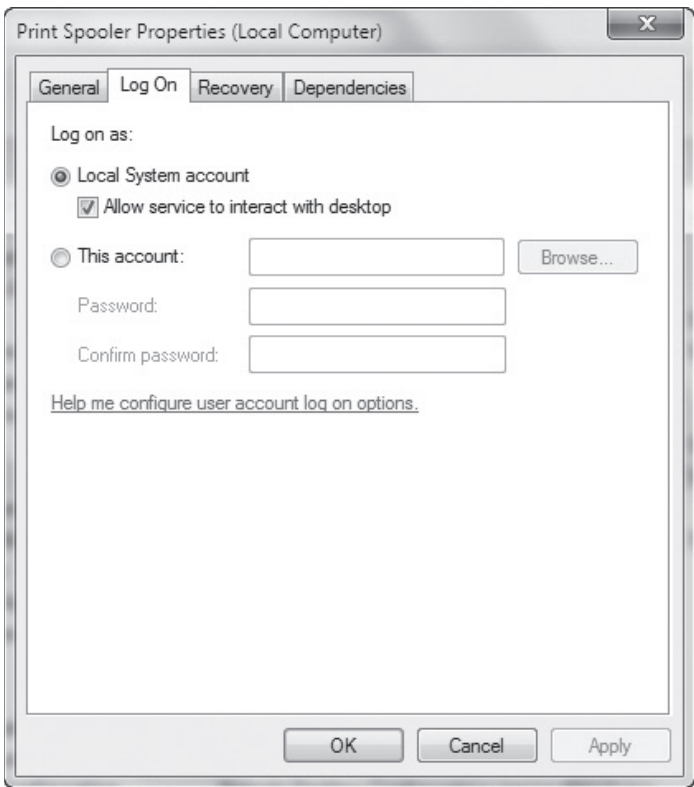
3.4

The Log On tab (see Figure 4-6) allows you to specify the user account the service can use, which might be different from the logged-on user or the default computer account. Your options are:

- **Local Service account:** Click *This account* and then type **NT AUTHORITY\LocalService**. The Local Service account is a built-in account (it's already created in the operating system). It can run services in the background but has limited access to resources and objects, which helps protect the system if individual services are compromised. No password is required.
- **Network Service account:** Click *This account* and then type **NT AUTHORITY\NetworkService**. The Network Service is similar to the Local Service account but is geared for networking services. Like the Local Service account, the Network Service account can run services in the background but it helps to protect the computer from compromise.
- **Another account:** Click *This account*, click *Browse*, browse for a different user account, select it, and then click *OK*. Type the password for the user account you selected and then click *OK*.

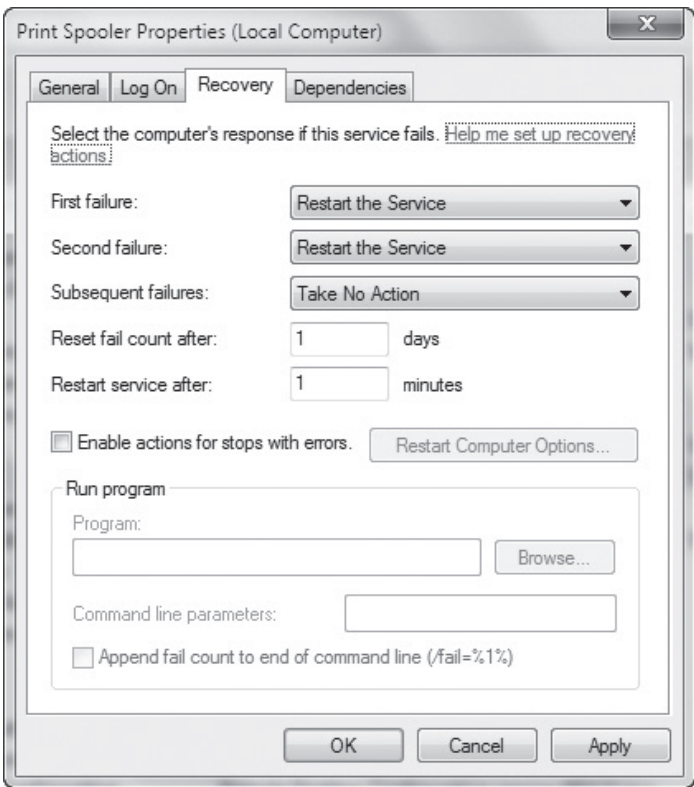
The service will run in the security context of the account you choose.

Figure 4-6
The Log On tab



The Recovery tab (see Figure 4-7) lets you choose recovery actions the computer will take if a service fails. For example, if a service fails, the computer might first try restarting the service. If that doesn't work, you can instruct the computer to restart the service again or you can restart the computer to clear memory and refresh connections.

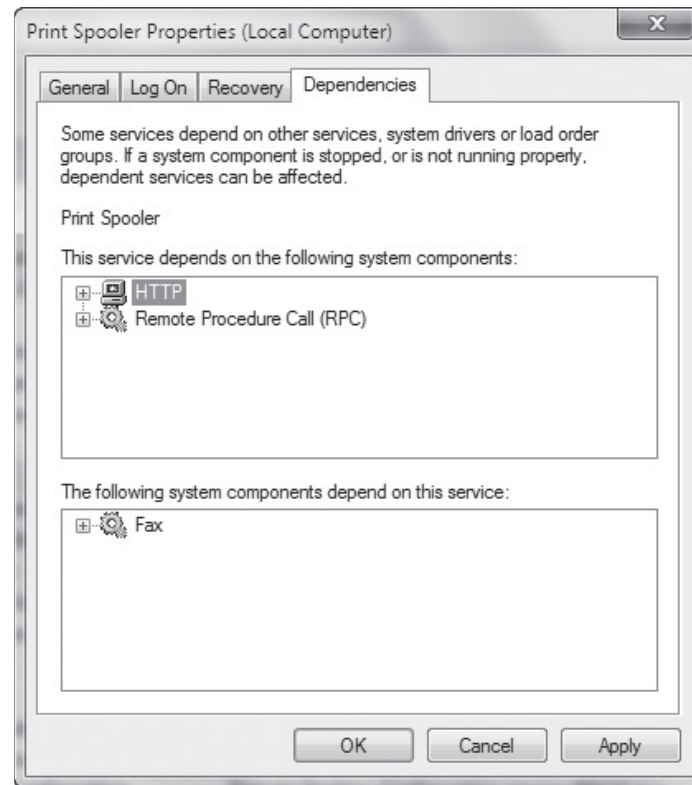
Figure 4-7
The Recovery tab



CERTIFICATION READY
What is a service
dependency?
3.4

The Dependencies tab (see Figure 4-8) shows you which services depend on other services to run. A dependent service starts after the service upon which it depends starts. Stopping a service also stops any other service that depends on it. There are no options available on this tab—it's informational only. However, before you stop or disable a service on the General tab, you should view the information on the Dependencies tab to know which other services might be affected by your change.

Figure 4-8
The Dependencies tab



CONFIGURE A SERVICE

GET READY. To configure a service in the Services console, perform the following steps:

1. Click **Start** and in the **Search programs and files** search box, type **services**, right-click **services.msc** in the resulting list, select **Run as administrator**, click **Yes** to continue (or type a password), and then press **Enter**.
2. In the details pane, double-click the service that you want to configure, such as **Print Spooler** (see Figure 4-9). The service's Properties dialog box displays.
3. On the General tab, click the **Startup type** drop-down list (see Figure 4-10). Select **Automatic (Delayed Start)**, **Automatic**, **Manual**, or **Disabled**.
4. Click the **Log On** tab. To specify the user account that the service can use to log on, perform one of the following steps:
 - To use the Local System account, click **Local System** account.
 - To use the Local Service account, click **This account** and then type **NT AUTHORITY\LocalService**.
 - To use the Network Service account, click **This account** and then type **NT AUTHORITY\NetworkService**.
 - To specify another account, click **This account**, click the **Browse** button, and then specify a user account in the Select User dialog box that displays. Click **OK** to save your changes and close the dialog box.

Figure 4-9
The Print Spooler service in the Services console

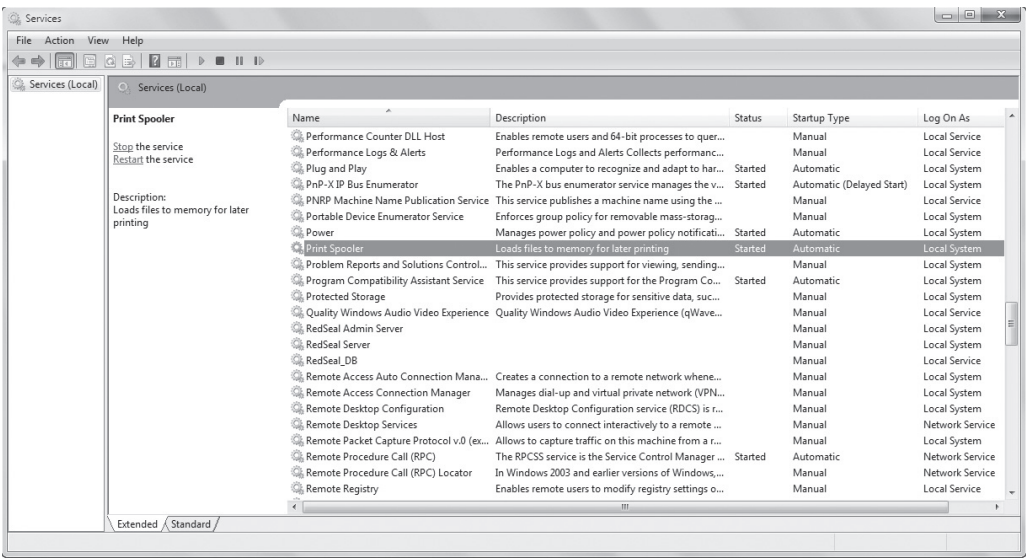
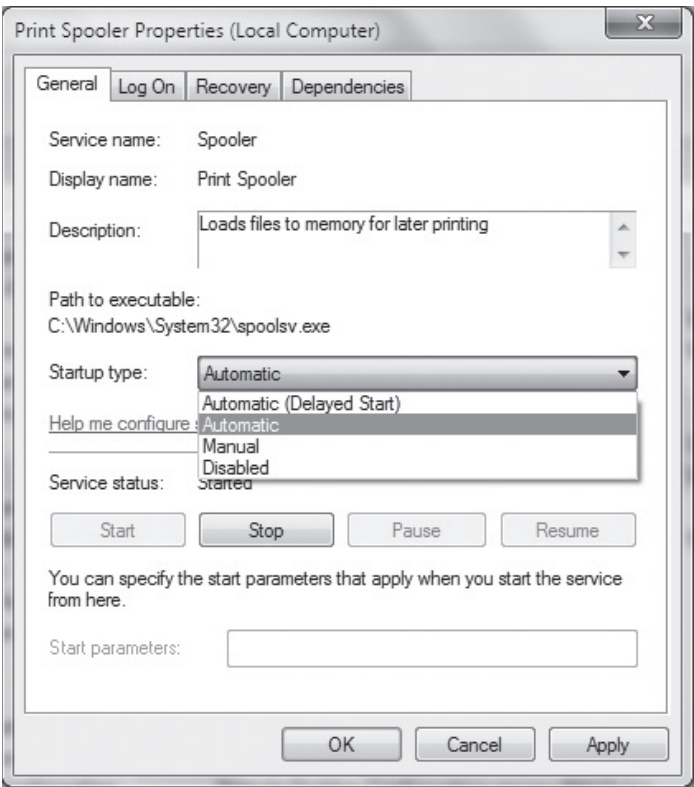


Figure 4-10
Selecting a startup type



5. Type the password for the user account in the **Password text box** and the **Confirm password** text box, and then click **OK**. You do not have to type a password if you selected the Local Service account or Network Service account.

+ MORE INFORMATION

For more information about Windows 7 services, visit [http://msdn.microsoft.com/en-us/library/windows/desktop/ms685141\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms685141(v=vs.85).aspx)

■ Using MSCONFIG (System Configuration utility)



THE BOTTOM LINE

Use MSCONFIG, also known as the System Configuration utility, to troubleshoot and diagnose startup problems.

MSCONFIG, also known as the *System Configuration utility*, lets you enable or disable startup services, set boot options such as booting into Safe Mode, access tools like Action Center and Event Viewer, and more. You'll use this utility mainly to troubleshoot startup problems with Windows.

Understanding MSCONFIG

To open System Configuration, click Start, type **msconfig** in the *Search programs and files* search box, and then click msconfig.exe from the resulting list. The System Configuration window displays, showing the General tab (see Figure 4-11). Normal startup is selected by default (unless you've previously changed startup settings). A normal startup runs all device drivers and services. Other options include the following:

- **Diagnostic startup:** Runs basic devices and services only; equivalent to starting the computer in Safe Mode.
- **Selective startup:** Starts the system with some or all system services and startup items disabled.

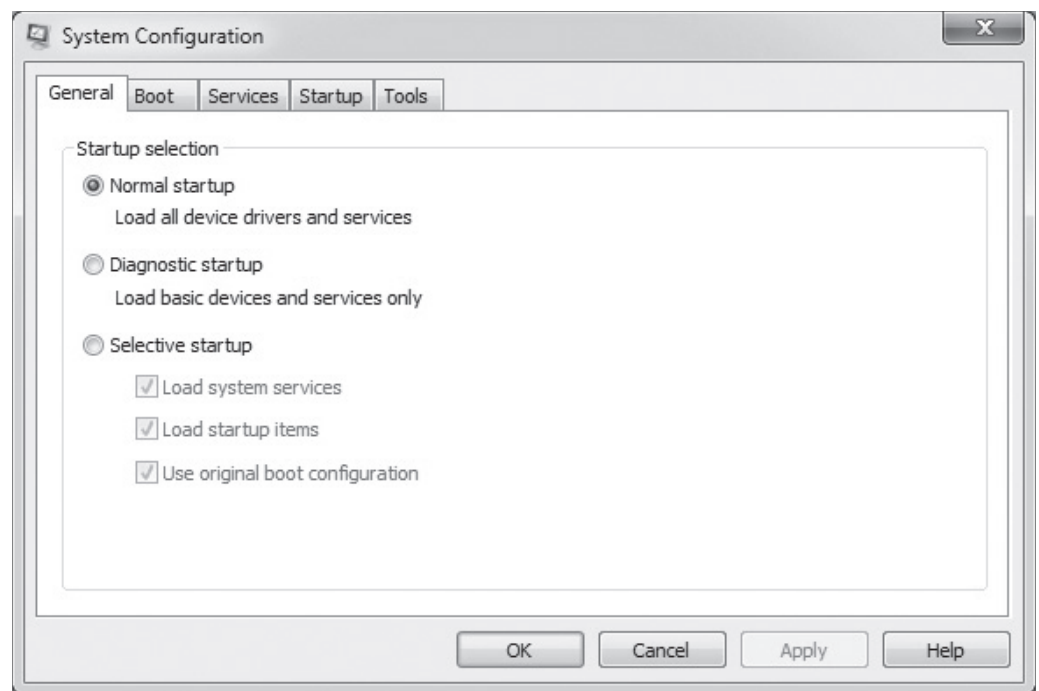
CERTIFICATION READY

What is the purpose of MSCONFIG?

1.3

Figure 4-11

The General tab



The options on the Boot tab (see Figure 4-12) enable you to adjust boot options, usually for diagnostic purposes. The Boot tab options match the options in the Advanced boot configuration menu that displays when you press F8 at startup. To boot the system into Safe Mode, select the

Safe boot check box. When you do this, the Minimal option is selected by default. The other safe boot options are:

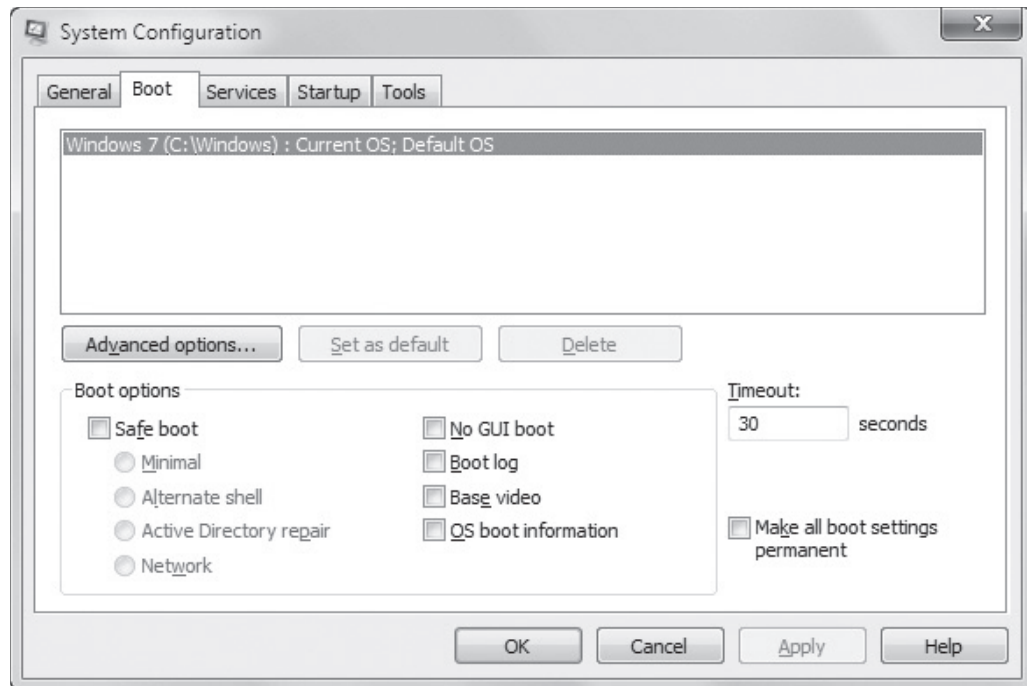
- **Alternate shell:** Boots to the command prompt without network support.
- **Active Directory repair:** Boots to the Windows GUI and runs critical system services and Active Directory.
- **Network:** Boots into Safe Mode with network services enabled.

The options in the right column are as follows:

- **No GUI boot:** Disables the Windows Welcome screen.
- **Boot log:** Creates a boot log of startup activity in a file named nbtlog.txt.
- **Base video:** Starts the Windows graphical user interface using standard VGA drivers.
- **OS boot information:** Displays driver names as drivers are installed during the startup process.

Figure 4-12

The Boot tab



TAKE NOTE *

You can make boot options permanent by selecting the *Make all boot settings permanent* check box, clicking Apply, and then clicking OK. Administrators often do this on test computers that they use to test new programs and updates before rolling them out to ordinary users.

You use the Services tab (see Figure 4-13) to enable or disable Microsoft and third-party services. These are the same services that display in the Services console covered earlier in this lesson.

The Startup tab (see Figure 4-14) allows you to enable or disable startup programs by selecting or deselecting the check boxes. The Startup tab lists the name of the startup item, its manufacturer, the path to and the name of its executable file, its location in the Windows registry, and the date it was disabled (if applicable).

Figure 4-13
The Services tab

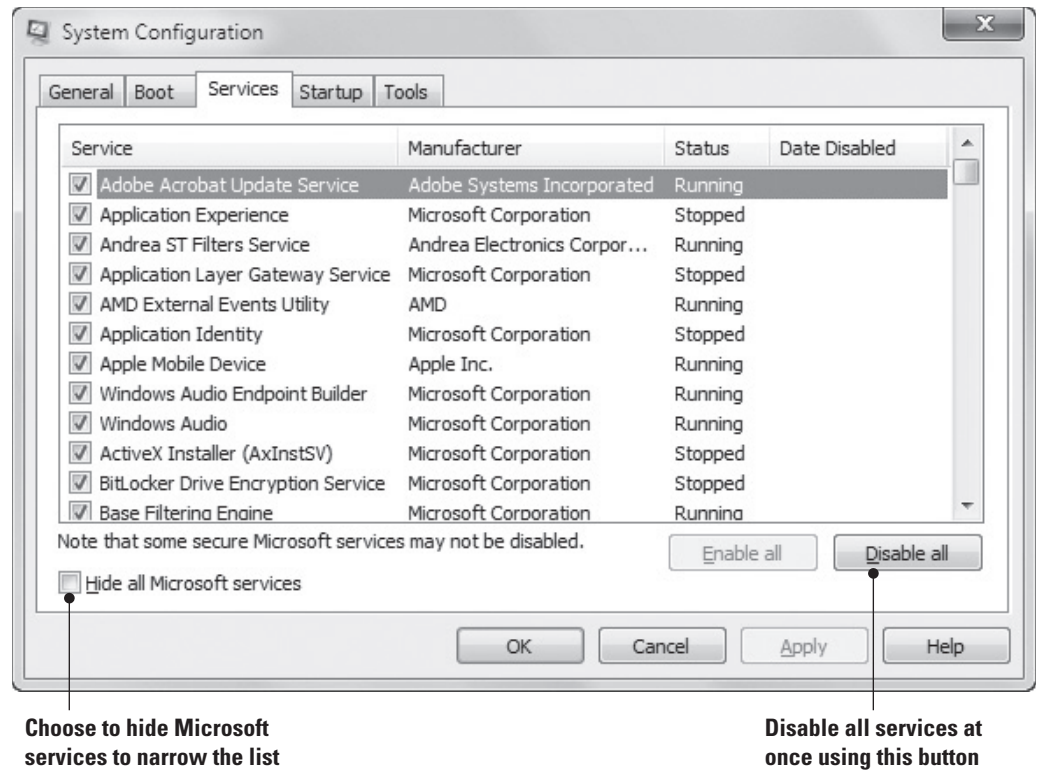
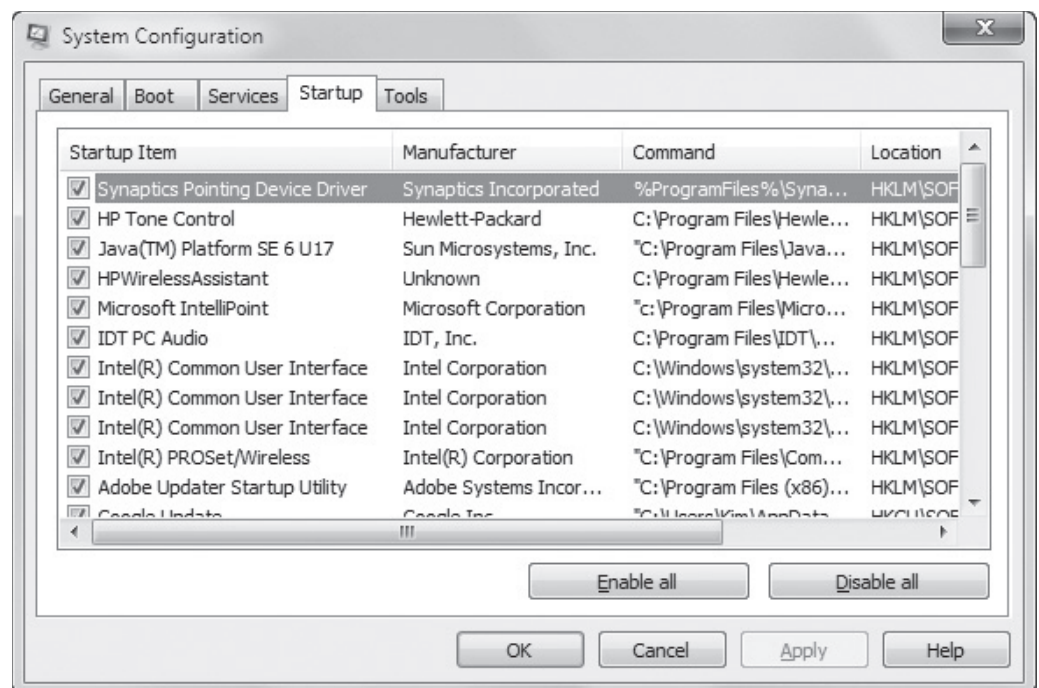


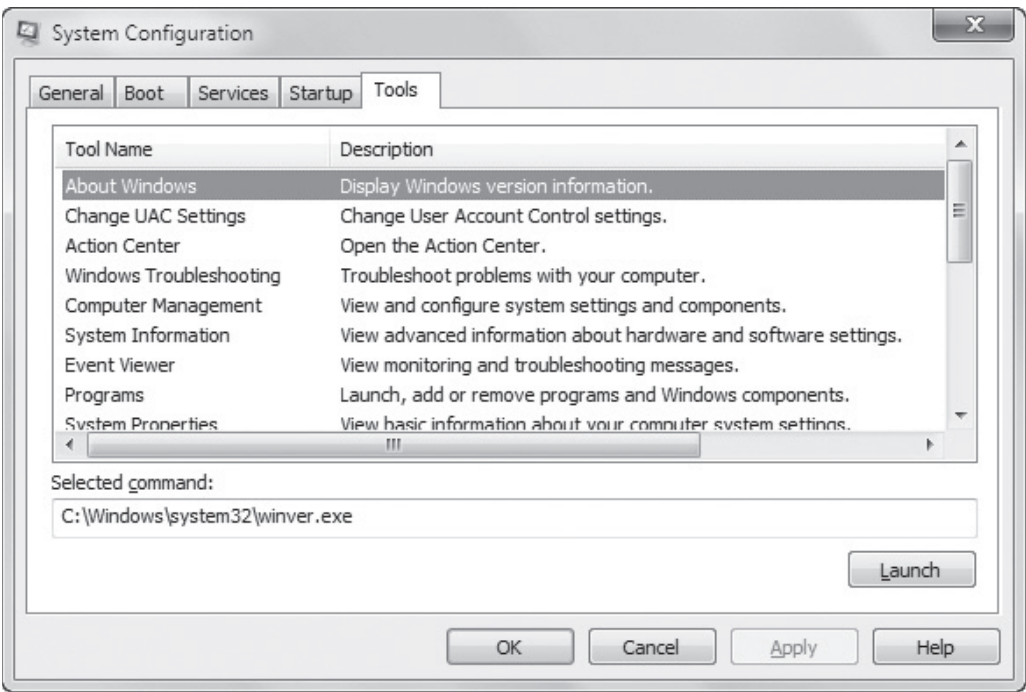
Figure 4-14
The Startup tab



Finally, the Tools tab (see Figure 4-15) lists many programs you can start for reporting and diagnostic purposes. Some of the tools are Change UAC Settings, Event Viewer, Performance Monitor, and Task Manager.

Figure 4-15

The Tools tab



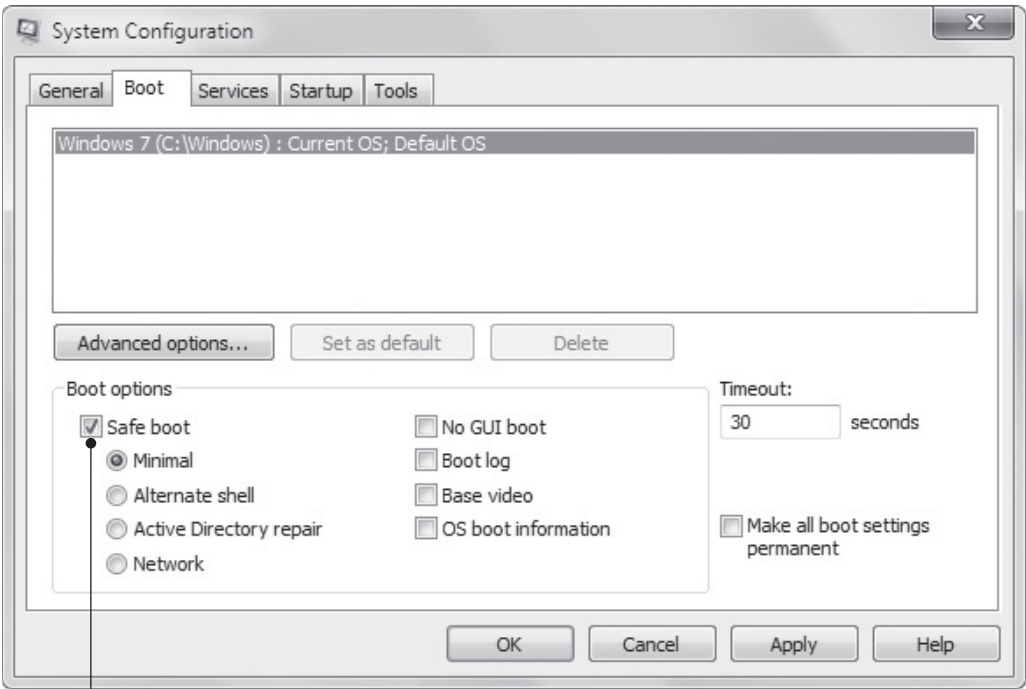
CHANGE SYSTEM CONFIGURATION SETTINGS

GET READY. To configure settings in the System Configuration utility, perform the following steps:

- 1. Open the System Configuration utility by clicking **Start**, typing **msconfig** in the **Search programs and files** search box, and then clicking **msconfig.exe** in the resulting list. Provide an administrative password or confirm to continue, when prompted.
- 2. Click the **Boot** tab, select the **Safe boot** check box (see Figure 4-16), and then click **OK**.
- 3. Restart your computer. The computer starts in Safe Mode.

Figure 4-16

Selecting the Safe boot option on the Boot tab



Safe boot option

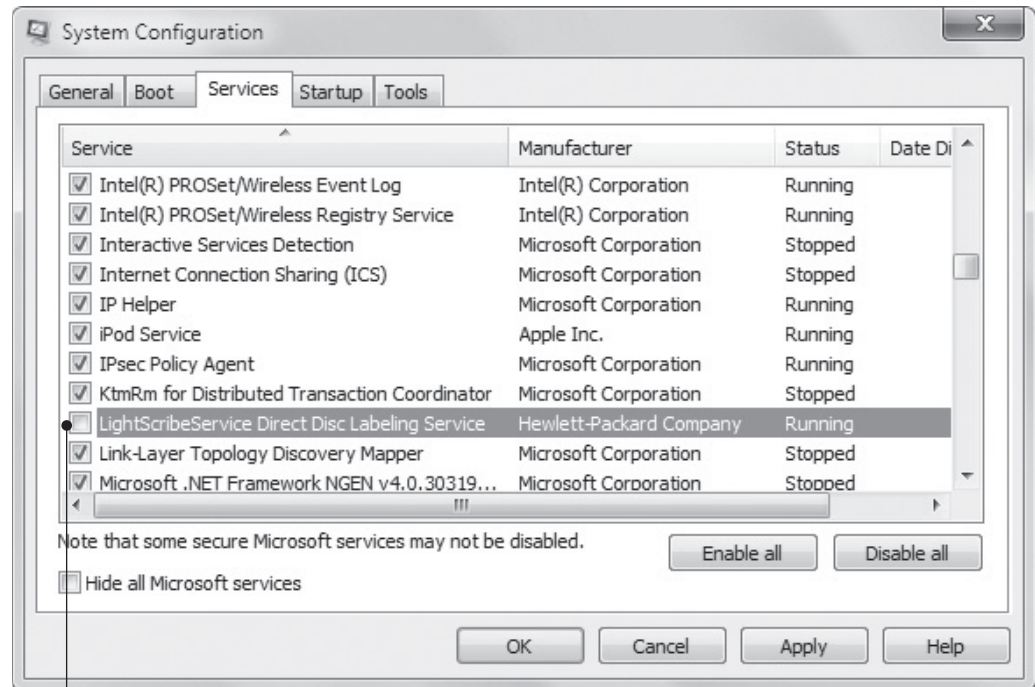
TAKE NOTE *

Clicking a column heading arranges the entries in alphabetical order.

4. Open the System Configuration utility, click the **Boot** tab, deselect the **Safe boot** check box, click **OK**, restart your computer, and then return to the System Configuration utility.
5. Click the **Services** tab. Browse the list of services and select a service that is not needed on your PC. In this example, we use the LightscribeService Direct Disc Labeling Service because it's seldom, if ever, used. Deselect the check box to the left of the service name (see Figure 4-17). Click **Apply**.

Figure 4-17

Disabling an unneeded service

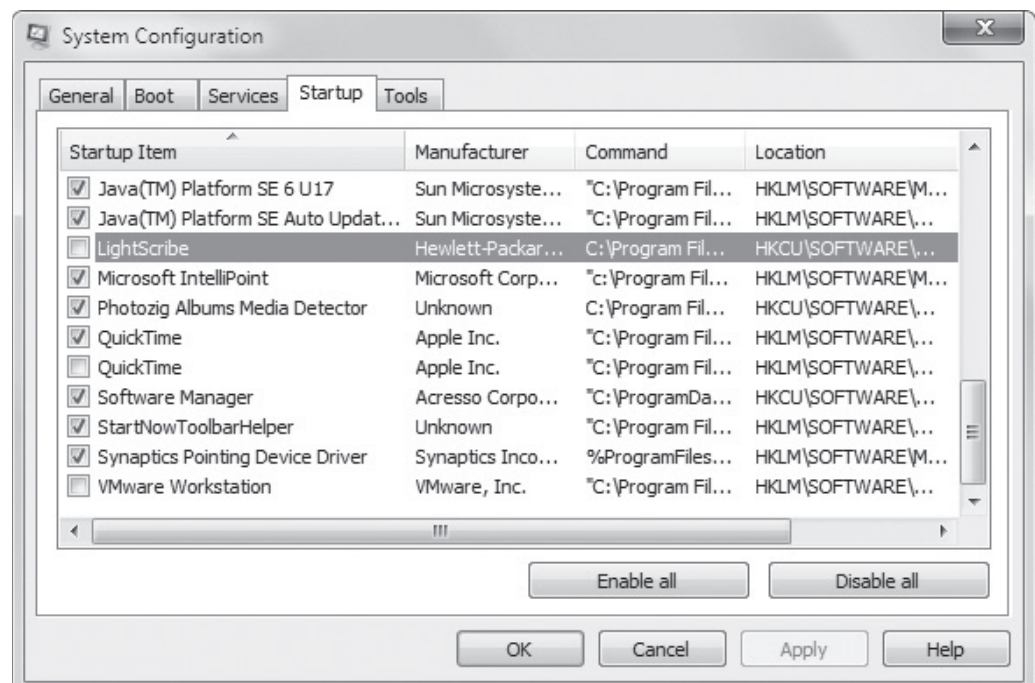


Deselect a service to disable it

6. Click the **Startup** tab. Browse the list of startup items and deselect an item that you don't want to start when your computer starts. In our example (see Figure 4-18), we deselected the Lightscribe program. Click **Apply**.

Figure 4-18

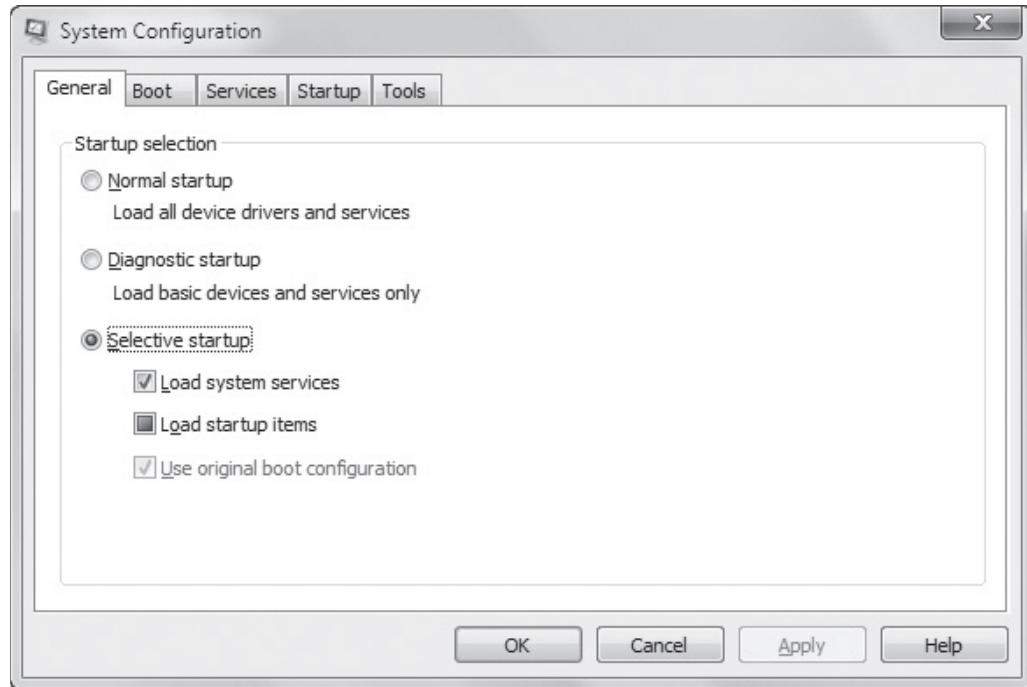
Disabling an unneeded startup item



7. Click the **General** tab and notice (see Figure 4-19) that **Selective startup** is now selected (instead of the Normal startup setting).

Figure 4-19

Selective startup enabled



8. Click **OK** to close the System Configuration utility.

If you have any problems with your system after disabling a service or startup item, return to the System Configuration utility and enable the service or startup item.

+ MORE INFORMATION

For more information about System Configuration, visit <http://windows.microsoft.com/en-US/windows-vista/Using-System-Configuration>

■ Understanding File Systems



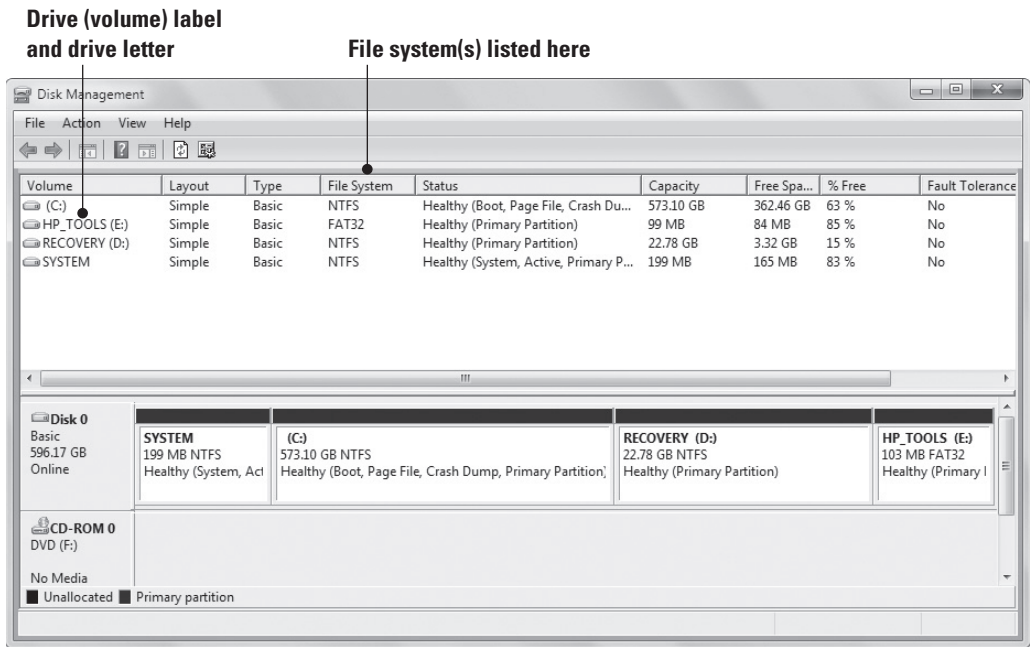
THE BOTTOM LINE

The three primary types of file systems for Windows are FAT, FAT32, and NTFS. It's best to use NTFS-formatted disks for Windows Vista and Windows 7 because NTFS handles small to very large hard disks, provides better security, and is the most reliable.

A **file system** is the overall structure your computer uses to name, store, and organize files and folders on a hard disk or partition. The file system provides a map of the clusters (the basic units of logical storage on a hard disk) that a file has been stored in. When you install a hard disk in a computer, you must format it with a file system. Today, the primary file system choices for a computer that will run Windows are NTFS, FAT32, and FAT. In Windows 7, you can view file systems in use on your computer from the Disk Management MMC snap-in (see Figure 4-20).

Figure 4-20

The Disk Management MMC snap-in displays disks and partitions as well as the file system in use



Understanding FAT, FAT32, and NTFS

Most Windows Vista and Windows 7 users use *NTFS* because it supports larger disks (up to 256 terabytes [TB]!) than FAT32 or FAT, and NTFS-formatted files and folders provide better security. It's also more reliable, with built-in features for recovering from disk errors automatically. Microsoft recommends NTFS for its security features: You can use encryption and permissions to restrict file access to specific users.

FAT32 and *FAT* (which is seldom used today) were popular in earlier versions of Windows (such as Windows 95, Windows 98, Windows Millenium Edition, Windows NT, and Windows 2000). The limitations of FAT32 make it less desirable than NTFS:

- A FAT32 partition is limited to a maximum size of 32 gigabytes (GB).
- The maximum size of a file that can be stored on a FAT32 volume is 4 GB.

So why use FAT32? Many universal serial bus (USB) flash drives come formatted as FAT32 to be compatible with a large variety of operating systems. If you plan to configure your computer for *multi-booting*, where you choose at startup which operating system you want to load, you might need to format a partition with FAT32 if that partition will run Windows 95, Windows 98, or Windows Millenium Edition.

Table 4-1 compares attributes of FAT, FAT32, and NTFS.

Table 4-1
Comparing FAT, FAT32, and NTFS

FILE SYSTEM	MAXIMUM PARTITION SIZE	MAXIMUM FILE SIZE
FAT	2 GB	2 GB
FAT32	32 GB	4 GB
NTFS	256 TB	Limited by size of volume on which it resides

CERTIFICATION READY
What are the differences between FAT, FAT32, and NTFS?
4.1

TAKE NOTE *
You can view all available disks in the Windows Computer folder in the Hard Disk Drives section.

You can usually convert a FAT or FAT32 partition to NTFS with few to no problems. One hitch you might run into is if the disk is nearly full. The conversion process (Convert.exe) needs a certain amount of free disk space to work properly. If there is insufficient free disk space, Convert.exe will notify you.

TAKE NOTE *

Converting to NTFS is a one-way process. After you convert a drive to NTFS, you cannot convert it back to FAT or FAT32. You can reformat an NTFS drive to FAT32, but you would need to back up all of your data first and then copy it back.

You can also convert to FAT32 from a different type of file system, although you need to keep the FAT32 size limitations in mind. If the partition you want to format is larger than 32 GB, the conversion process won't be successful.

Before converting a disk from one file system to another, back up your data, if possible. If you have a relatively small number of files on a disk, and no system files or programs installed, it's better to back up the data to a different storage medium and then format the disk.



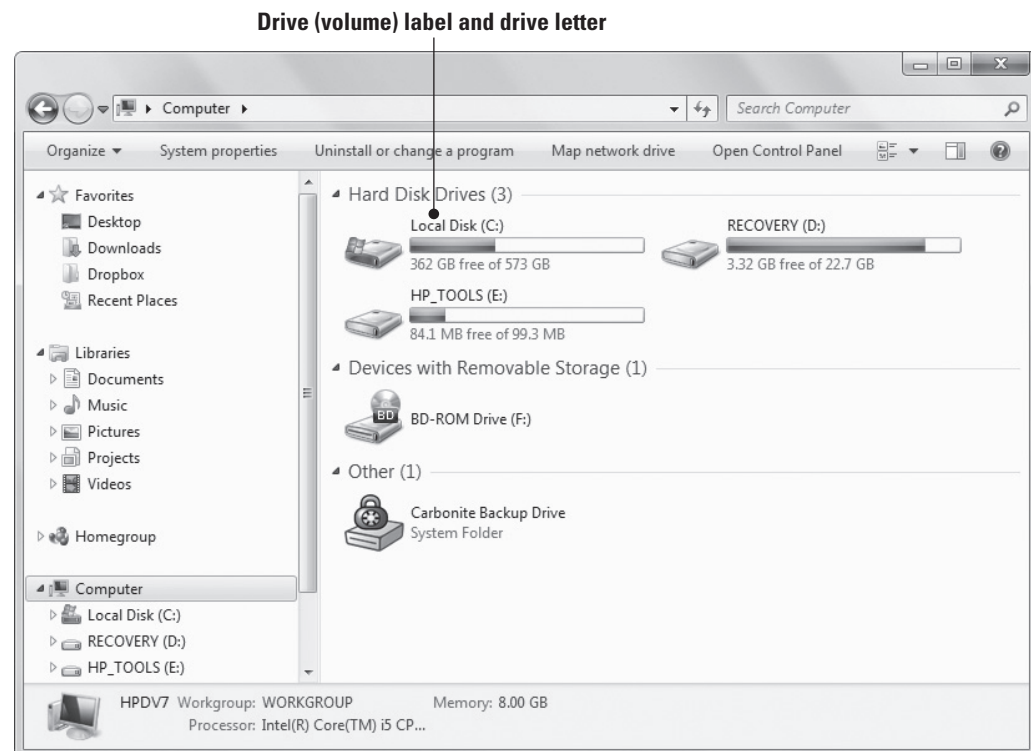
CONVERT A HARD DISK TO NTFS

GET READY. To convert a hard disk to NTFS format, perform the following steps:

1. Click **Start > Computer**. In the Computer window (see Figure 4-21), note the name of the drive you want to convert and the volume label. You can also get this information from the Disk Management snap-in.

Figure 4-21

The Computer window

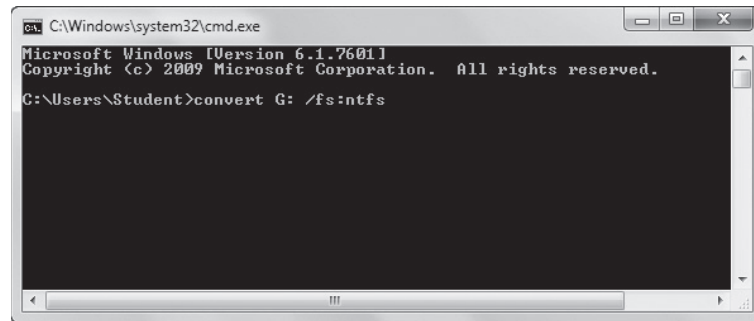


2. Close the Computer window and make sure no programs are running, including anti-virus and firewall programs. You should disconnect your computer from the Internet as a safety precaution.

3. Click **Start**, type **cmd** in the **Search programs and files** search box, right-click **cmd.exe** in the resulting list, and then select **Run as administrator**. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.
4. At the command prompt, type **convert drive_letter: /fs:ntfs**, where **drive_letter** is the letter of the drive you want to convert. (See Figure 4-22.) Press **Enter**. For example, typing **convert G: /fs:ntfs** and pressing Enter converts drive G to NTFS.

Figure 4-22

The convert command in a command-prompt window



5. A message displays, prompting you for the volume label. Type the volume label of the drive you're converting and press **Enter**.

The conversion begins and might take several minutes to more than an hour, depending on the size of the disk and the amount of data stored on it. A message displays when the conversion is finished. If the drive contains system files, you'll need to restart your computer before use.

+ MORE INFORMATION

To compare FAT32 and NTFS, go to <http://windows.microsoft.com/en-US/windows7/Comparing-NTFS-and-FAT32-file-systems>. To learn how to convert a hard disk or partition to NTFS, see <http://windows.microsoft.com/en-US/windows7/Convert-a-hard-disk-or-partition-to-NTFS-format>. For considerations when converting to FAT32 from a different file system, read <http://windows.microsoft.com/en-US/windows7/Convert-a-hard-disk-or-partition-to-FAT32-format>

■ Exploring and Managing Libraries



THE BOTTOM LINE

Libraries were introduced in Windows 7. A library looks like an ordinary folder, but it is a virtual folder that simply points to files and folders in different locations on a hard disk, network drive, or external drive.

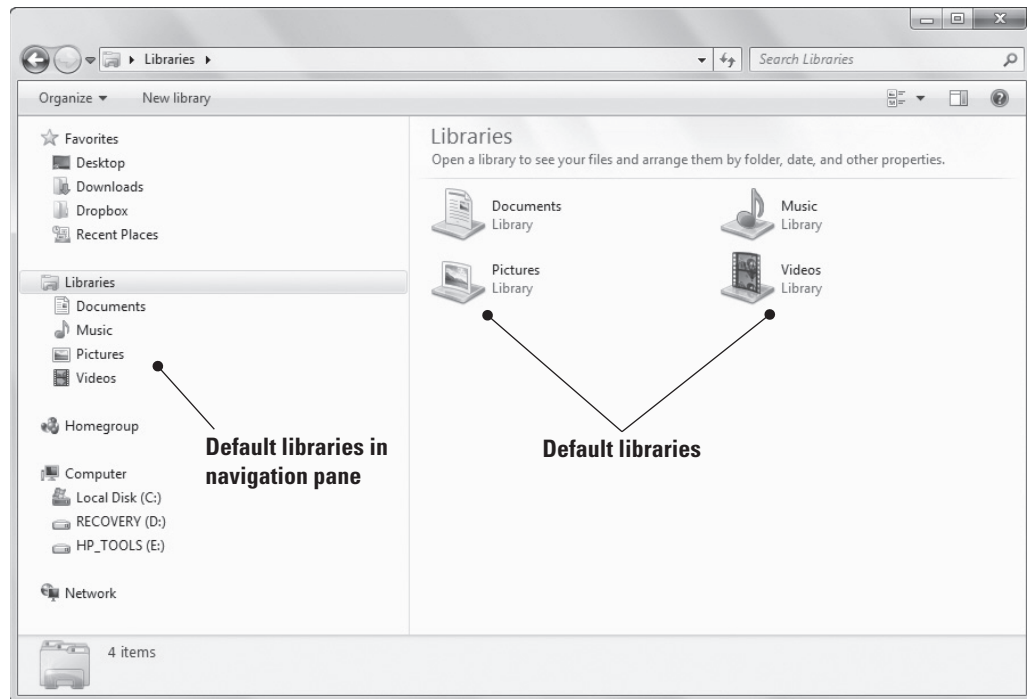
In Windows 7, a **library** is a virtual folder that can display content from different locations (folders, for example) on your computer or an external drive. A library looks like an ordinary folder but simply points to files and folders that are located elsewhere. You access libraries in Windows Explorer, just like you do files and folders.

Windows 7 includes several default libraries (see Figure 4-23):

- **Documents library:** Stores word-processing documents, spreadsheets, and similar files
- **Music library:** Stores audio files, such as those you've downloaded from the Web, transferred from a portable device (music player), or ripped from a CD
- **Pictures library:** Stores digital image files
- **Videos library:** Stores video files

Figure 4-23

Default libraries in Windows 7

**CERTIFICATION READY**

How are multiple local locations added to a library?

4.4

CERTIFICATION READY

How is a networked location added to a library?

4.4

X REF

Offline Files were covered in Lesson 3. The Windows 7 libraries FAQ, mentioned in the More Information bar at the end of this section, offers a pointer for getting help with search indexing.

Each default library contains a “My” folder that matches the library name. For example, the Documents library contains a My Documents folder, the Music library contains a My Music folder, and so on. Libraries and folders are unique for each Windows user account on a computer. For example, if three users share the same computer and each user has a user account, each has separate libraries and folders. Windows 7 stores data files in C:\Users\username.

Adding Local and Networked Locations to a Library

Want to create a new library, add local locations to a library, or add a networked location to a library? All of these tasks are easy to do.

When creating a new library, you must include at least one folder within the library for organizational purposes. You can then copy, move, or save files to the folder in the library.

You can add a location such as a folder on your C: drive, a second hard drive in your computer, or an external drive to an existing library. Just navigate to the folder in Windows Explorer, select it, click *Include in library* on the toolbar, and select the library to which you want to add the folder. You can also add multiple folders to a single library.

The same principal applies to networked locations. The only caveat with a networked location is that it must be added to the search index or be available offline before you can add it to a library.



ADD A FOLDER TO A LIBRARY

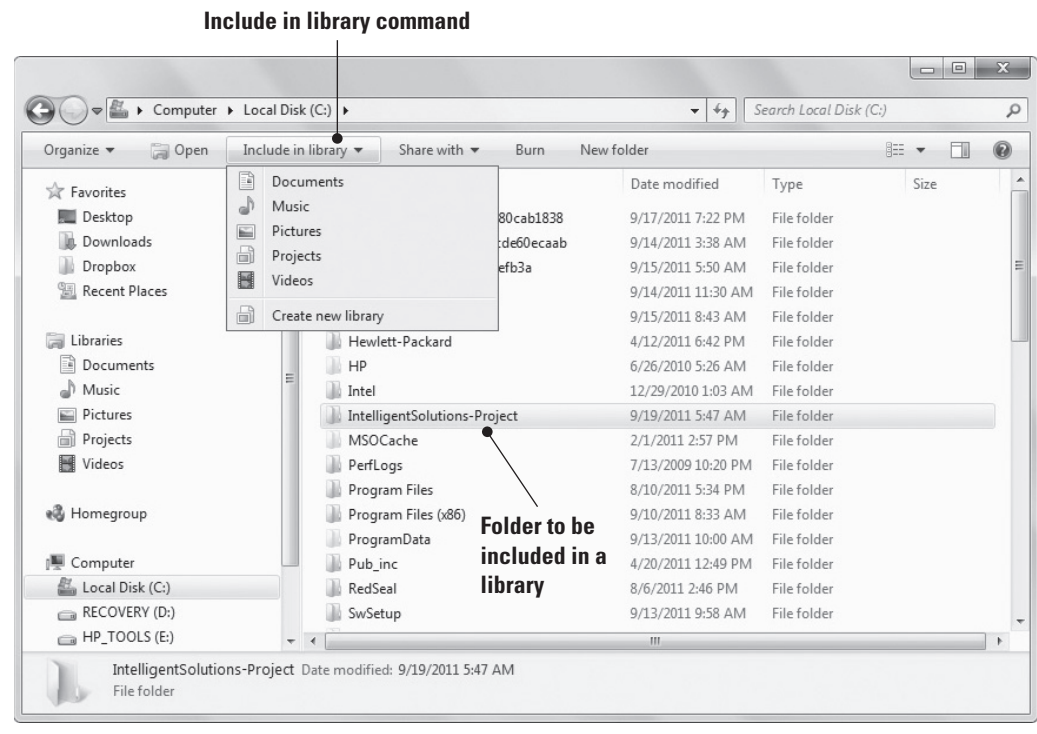
GET READY. To add a folder to a library, perform the following steps:

1. Click **Start > Computer**. Windows Explorer opens. (You can also open Windows Explorer by clicking **Start** and then clicking **Documents**.)

2. In Windows Explorer, use the navigation pane on the left to locate the folder you want to include in a library and click to select it. The folder cannot already be included in another library.
3. On the toolbar, click **Include in library** (see Figure 4-24), and then click a library (such as Documents, Music, Pictures, or Videos).

Figure 4-24

Selecting a library in which to include a folder



To include a folder on an external drive in a library, follow the previous steps but navigate to the folder on your external hard drive that you want to include. Make sure the external hard drive is connected to your computer and that your computer recognizes the device—it should be listed in Windows Explorer near your C: drive. You can't include content on removable media, such as a CD or DVD, in a library. Some USB flash drives devices don't work with libraries either.



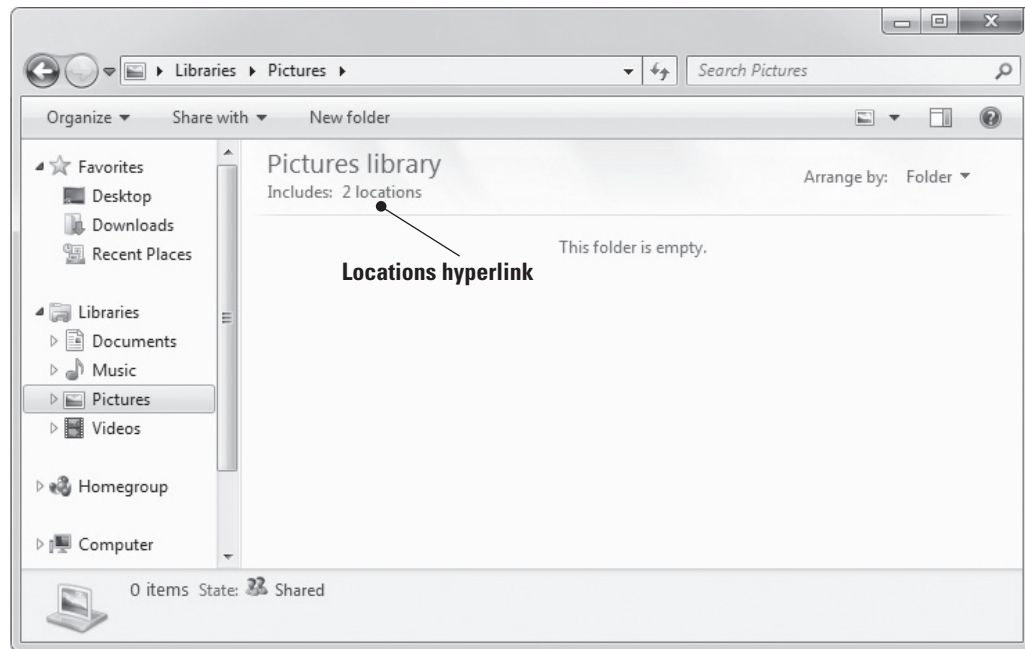
ADD A FOLDER TO THE PICTURES LIBRARY

GET READY. Adding photos from various locations to the Pictures library requires a few different steps. To add photos in a folder that's already in another library (such as Documents) to the Pictures library, perform the following steps:

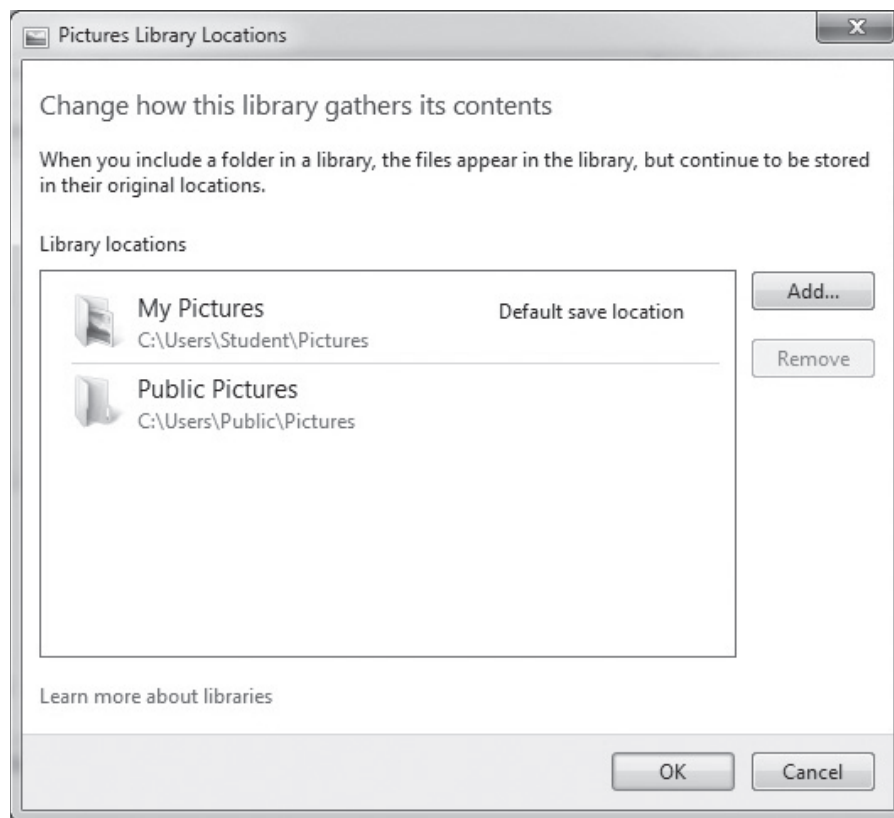
1. In Windows Explorer, navigate to and click the **Pictures** library to open it.
2. Click the locations hyperlink at the top of the main pane (see Figure 4-25).
3. The Pictures Library Locations dialog box displays (see Figure 4-26). Click **Add**.

Figure 4-25

The locations hyperlink is located at the top of the main pane

**Figure 4-26**

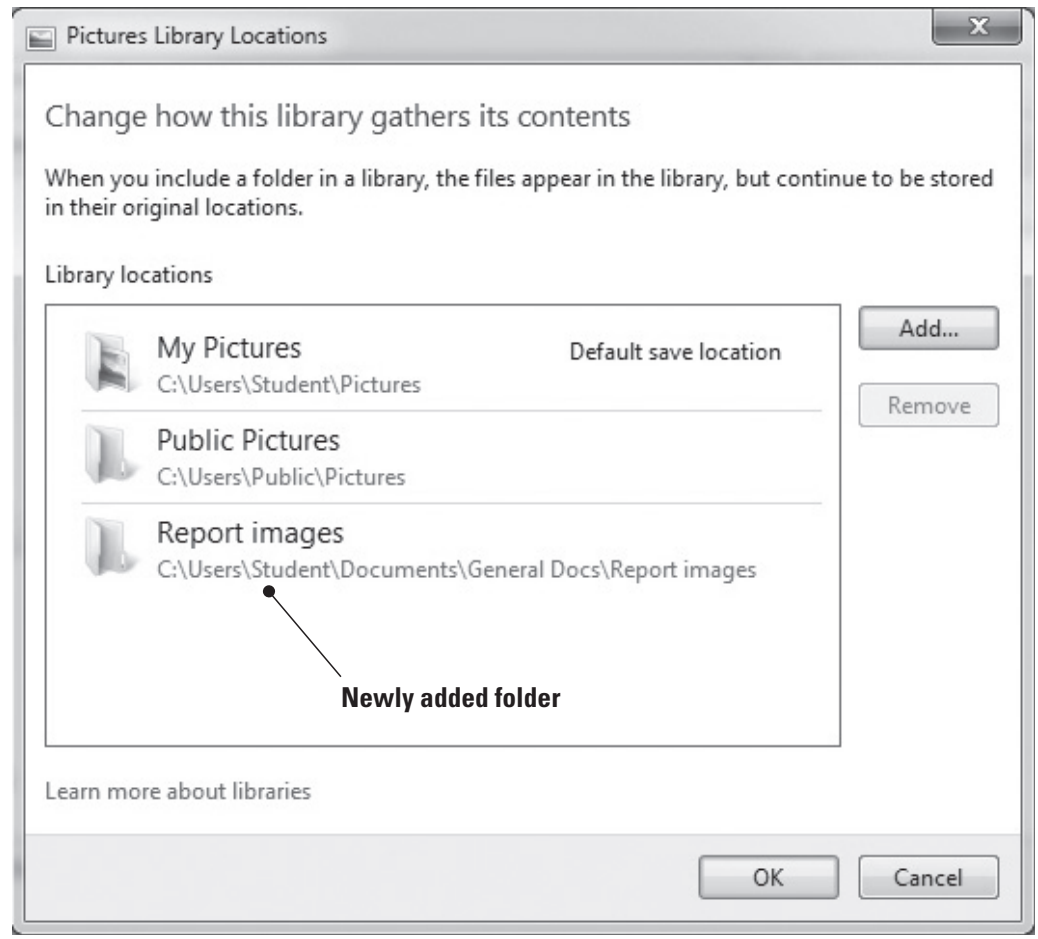
Pictures Library Locations dialog box



4. Navigate to the folder that contains the images you want to include in the Pictures library (in this example, a folder named "Report images"), click the folder, and then click **Include folder**.
5. The Pictures Library Locations dialog box displays the newly added folder (see Figure 4-27). Click **OK**.

Figure 4-27

Pictures Library Locations dialog box displaying a newly added folder



The photos remain in the original location, but can now be accessed from the Pictures library.



ADD A NETWORKED LOCATION TO A LIBRARY

GET READY. To add a networked location to a library, perform the following steps:

1. In Windows Explorer, in the navigation pane, click **Network**.
2. Navigate to the folder on your network that you want to include in a library on your computer.
3. On the toolbar, click **Include in library**, and then click a library.

Remember, content in a network location must be indexed for search or available offline in order to include it in a library.



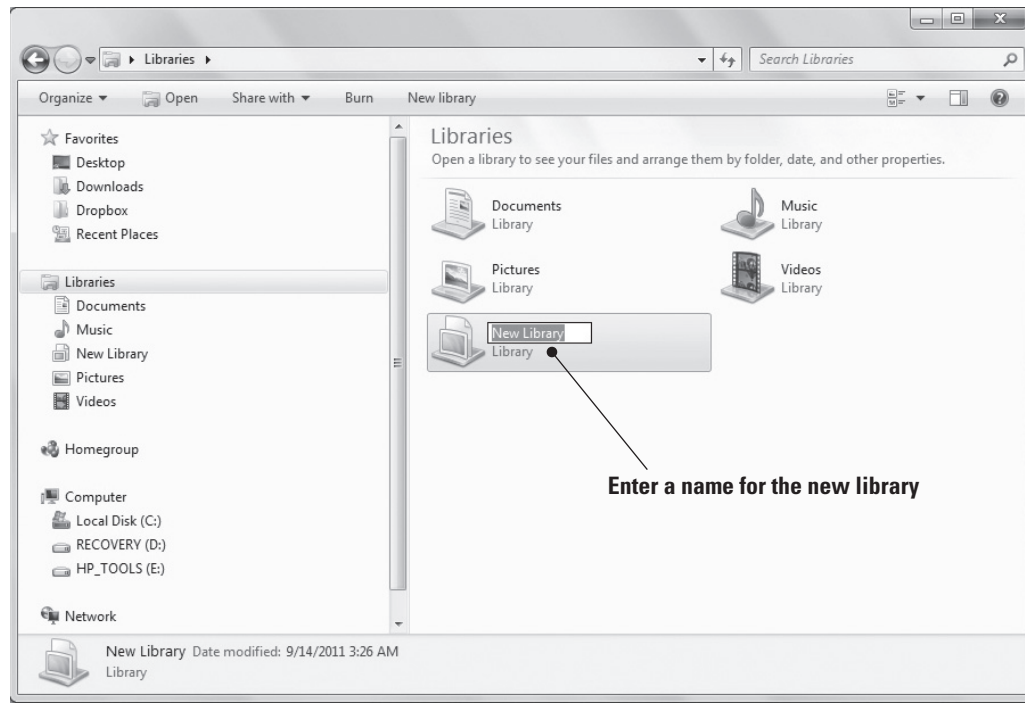
CREATE A NEW LIBRARY

GET READY. To create a new library, perform the following steps:

1. In Windows Explorer, in the navigation pane, click **Libraries** (unless Libraries is already displayed).
2. On the toolbar, click **New library**.
3. Type a name for the library (see Figure 4-28) and then press **Enter**.

Figure 4-28

Creating a new library



The newly created library has the same functionality as the default libraries. After double-clicking the new library to open it, click the *Include a folder* button, use the navigation pane to find a folder you want to include, click it, and then click *Include folder*.

+ MORE INFORMATION

For more information about Windows 7 libraries, visit <http://windows.microsoft.com/en-US/windows7/products/features/libraries>. You might also want to read the Windows 7 libraries FAQ at <http://windows.microsoft.com/en-US/windows7/Libraries-frequently-asked-questions>

■ Encrypting and Compressing Files and Folders



THE BOTTOM LINE

Encrypting files and folders protects them from unwanted access. Microsoft uses the Encrypting File System (EFS) to encrypt individual files and folders in Windows Vista and Windows 7.

TAKE NOTE *

Windows 7 Starter, Home Basic, and Home Premium do not fully support EFS.

Encryption protects the contents of files and folders from unauthorized access. Windows uses **Encrypting File System (EFS)** to allow users to encrypt information on hard disks, external flash disks, CDs, DVDs, backup tapes, and other types of physical media. Files and folders are not encrypted in Windows 7 by default; however, users can enforce encryption on data files, folders, and entire drives. Encrypted (EFS) files and folders are displayed in green in Windows Explorer.

CERTIFICATION READY

How are files and folders encrypted using Encrypting File System (EFS)?

4.3

Understanding Encrypting File System (EFS)

The data in an encrypted file is “scrambled” but still readable and usable by the user who encrypted the file; that user—and any other authorized users—can open and change the file as necessary. However, an unauthorized user who tries to open the file or copy it receives an

TAKE NOTE *

It's more efficient to encrypt at the folder level rather than the file level. New files added to the folder will also be encrypted.

TAKE NOTE *

Encrypted files can be significantly larger than unencrypted files, and the encryption/decryption process can add significant processing overhead.

"Access Denied" message. Only the original owner and the computer's designated recovery agent can access encrypted files. The designated recovery agent is the Administrator account, by default, on a local computer or in a domain.

A file created in or moved to an encrypted folder is automatically encrypted. The folder itself isn't encrypted; however, a user with appropriate file access permissions can see the names of the files in the folder.

When you mark a file for encryption, Windows generates a large, random number—a unique **encryption key**. The key is used to scramble the contents of the file. This encryption key is also encrypted with a personal file encryption certificate, which is stored in the Windows Certificate database. The file's encryption key is stored along with the file.

When you're logged on to Windows and attempt to open an encrypted file, Windows retrieves your personal **EFS certificate**, decodes the file's unique encryption key, and uses that key to decode the contents of the file.

If you lose an encryption key or your EFS certificate, or one of them becomes damaged, you could lose your data. It's important to back up your encryption key(s) and certificate and keep them in a safe place. You should also consider creating a file recovery certificate.



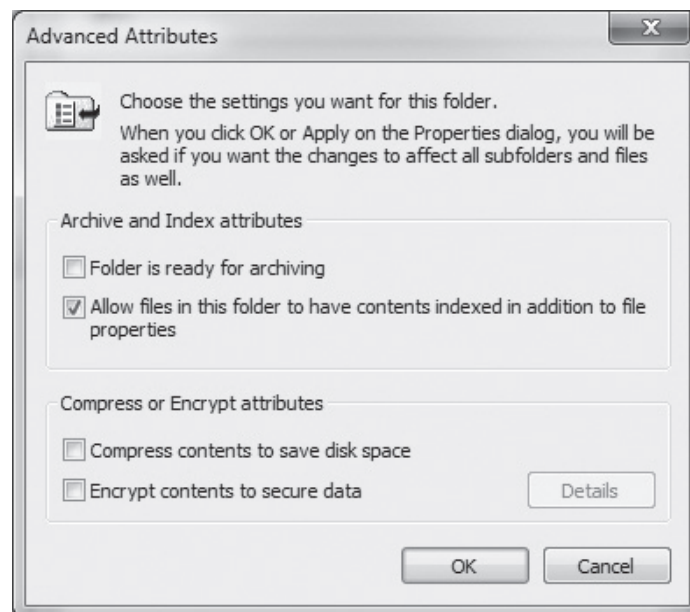
ENCRYPT A FILE OR FOLDER

GET READY. To encrypt and decrypt a file or folder, perform the following steps:

1. In Windows Explorer, right-click the file or folder you want to encrypt, and then click **Properties**. The Properties dialog box displays.
2. On the **General** tab, click **Advanced**. The Advanced Attributes dialog box displays (see Figure 4-29).

Figure 4-29

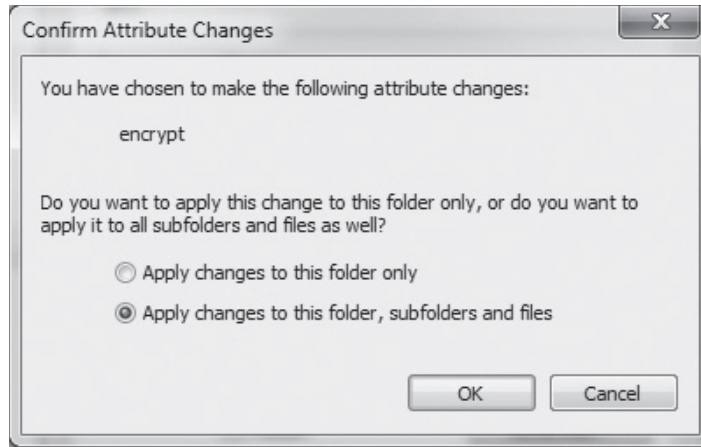
The Advanced Attributes dialog box



3. Select the **Encrypt contents to secure data** check box, and then click **OK**.
4. Click **OK** to accept your settings and close the Properties dialog box.
5. The Confirm Attribute Changes dialog box displays (see Figure 4-30). Choose either **Apply changes to this folder only** or **Apply changes to this folder, subfolders and files**.

Figure 4-30

The Confirm Attribute Changes dialog box



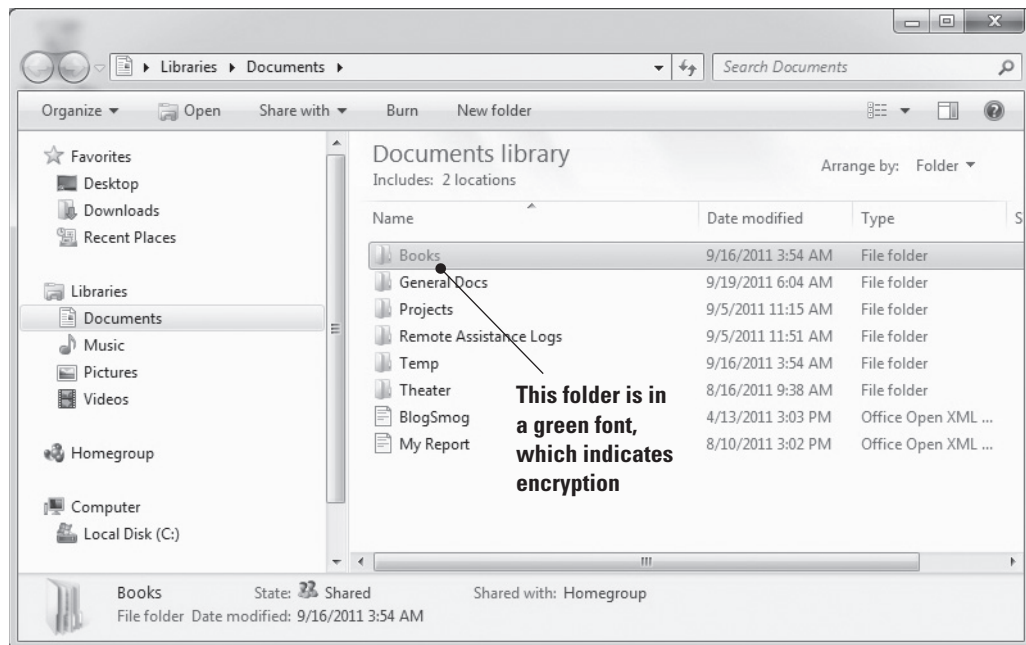
6. Click **OK**.

As Windows encrypts the folder, you are reminded to back up your encryption key. Microsoft recommends that you back up the encryption key immediately. Click the balloon reminder and follow the prompts.

An encrypted folder displays in green in the Windows Explorer file list (see the Books folder in Figure 4-31) so you can see at a glance that it's encrypted.

Figure 4-31

An encrypted folder displays in green in the file list



DECRYPT A FILE OR FOLDER

GET READY. To decrypt a file or folder, perform the following steps:

1. Right-click the file or folder you want to decrypt, and then click **Properties**.
2. Click the **General** tab, and then click **Advanced**.
3. Deselect the **Encrypt contents to secure data** check box, and then click **OK**.



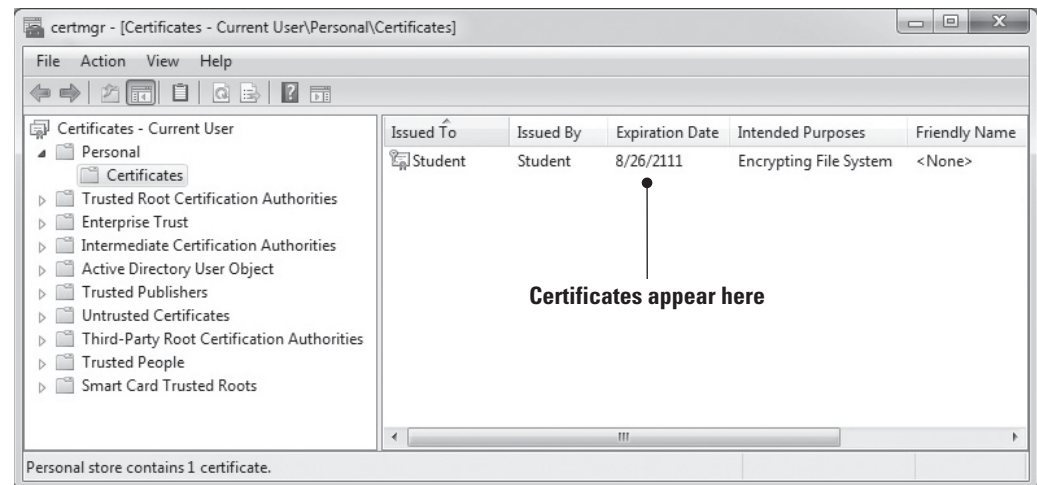
BACK UP YOUR EFS CERTIFICATE

GET READY. To back up your EFS certificate, perform the following steps:

1. Click **Start** and in the **Search programs and files** search box, type **certmgr.msc** then click **certmgr** in the resulting list. The Certificate Manager displays.
2. Expand the **Personal** folder by clicking its arrow.
3. Click **Certificates**. The user's personal certificates are listed (see Figure 4-32).

Figure 4-32

Personal certificates in Certificate Manager



4. Click the certificate that lists Encrypting File System in the **Intended Purposes** column. If there is more than one EFS certificate, select all of them.
5. Click the **Action** menu, point to **All Tasks**, and then click **Export**. The Export wizard starts.
6. Click **Next**.
7. Leave the **Yes, export the private key** option selected (see Figure 4-33) and then click **Next**.
8. Click **Personal Information Exchange**, and then click **Next**.
9. Type the password you want to use, confirm it, and then click **Next**.
10. The wizard creates a file to store the certificate. Click **Browse** and navigate to the location where you want to save the file, and then enter a name for the file. Click **Save**.
11. In the next screen, click **Next**.
12. Click **Finish**, and then click **OK**.

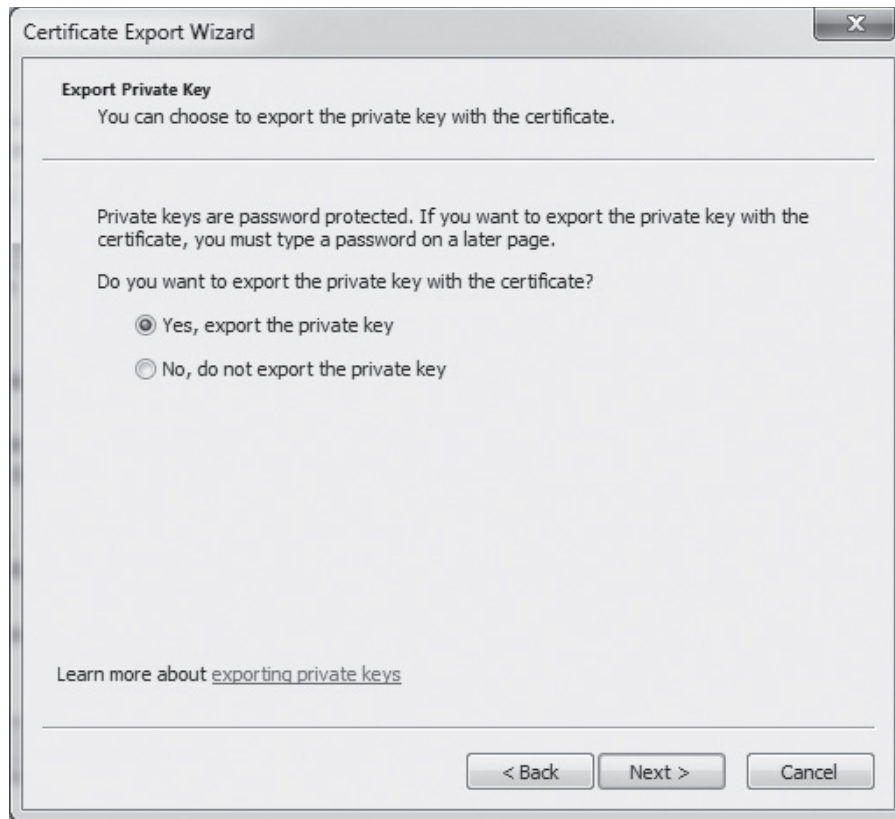
Be sure to back up the certificate file to a location that is different from where it's saved. For example, if you saved the file on your computer's hard disk, copy the file to removable media or a network location.

+ MORE INFORMATION

For details about EFS, visit <http://windows.microsoft.com/en-US/windows7/What-is-Encrypting-File-System-EFS>. To learn more about backing up an EFS certificate, go to <http://windows.microsoft.com/en-US/windows7/Back-up-Encrypting-File-System-EFS-certificate>

Figure 4-33

Using the Certificate Export Wizard



Understanding Compression

Compression allows you to save disk space by reducing the size of files and folders without affecting their content.

CERTIFICATION READY

How are files or folders compressed?

4.3

Compression is the process of decreasing the size of files or folders without affecting the files' content. The purpose of compression is to decrease large files that would otherwise use a lot of storage space. Because files often include a lot of redundant, repeated data, compressing them replaces repeated data with pointers to the data. The pointers take up much less space than the repeated data, so the size of the file is reduced.

TAKE NOTE *

You cannot encrypt files or folders that are compressed. If you want to encrypt a compressed file or folder, you must decompress it first.



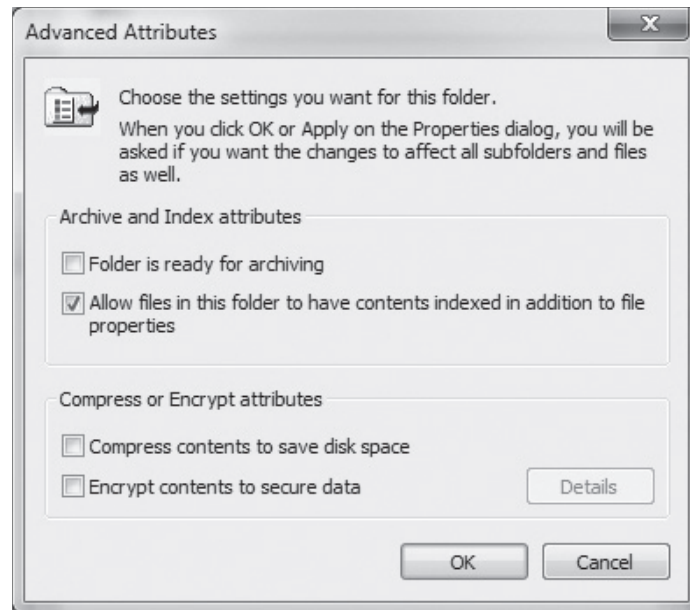
COMPRESS A FILE OR FOLDER

GET READY. To compress a file or folder, perform the following steps:

1. In Windows Explorer, right-click the file or folder you want to compress, and then click **Properties**. The Properties dialog box displays.
2. On the **General** tab, click **Advanced**. The Advanced Attributes dialog box displays (see Figure 4-34).
3. Select the **Compress contents to save disk space** check box, and then click **OK**.

Figure 4-34

The Advanced Attributes dialog box



The compressed file or folder displays in blue in Windows Explorer. To uncompress the file or folder, select it, return to the Advanced Attributes dialog box, and deselect the *Compress contents to save disk space* check box.

CERTIFICATION READY

What is the purpose of BitLocker?

4.3

CERTIFICATION READY

How does BitLocker encrypt and protect a hard drive?

5.2

Understanding BitLocker

BitLocker Drive Encryption encrypts an entire fixed disk to prevent access by unauthorized users. BitLocker To Go protects removable drives, such as external flash drives. You can encrypt drives with BitLocker in Windows Ultimate and Enterprise editions only.

BitLocker Drive Encryption is another method of protecting data stored on a fixed drive in a Windows computer. BitLocker encrypts the entire drive, rather than individual files and folders. The complementary BitLocker To Go protects data on removable data drives, such as an external flash drive.

TAKE NOTE *

BitLocker encryption is available in Windows 7 Ultimate and Enterprise editions, not in Professional, Home Premium, or Starter.

When you add new files to a BitLocker-encrypted disk, the files are encrypted automatically. If you copy the files to another drive, BitLocker automatically decrypts the files, which means they're no longer protected.

Anytime you start a computer on which the operating system disk is BitLocker-encrypted, BitLocker scans the drive for security risks. If BitLocker detects a potential security risk such as a change to the startup files, it locks Windows (prevents it from running) and requires the user to provide the BitLocker recovery key to unlock Windows. This ensures that unauthorized users cannot access the system to steal files or somehow damage the system or data.

Some computers have a Trusted Platform Module (TPM) chip on the motherboard. If the chip is present, BitLocker uses the TPM chip to protect the BitLocker keys. When a user starts a computer with a TPM chip and with BitLocker enabled, BitLocker requests the keys from the TPM and unlocks the system.

TAKE NOTE*

BitLocker Drive Encryption encrypts an entire drive. EFS protects individual files and folders on any drive on a per-user basis.

You can turn off BitLocker at any time by suspending it temporarily or decrypting the drive.

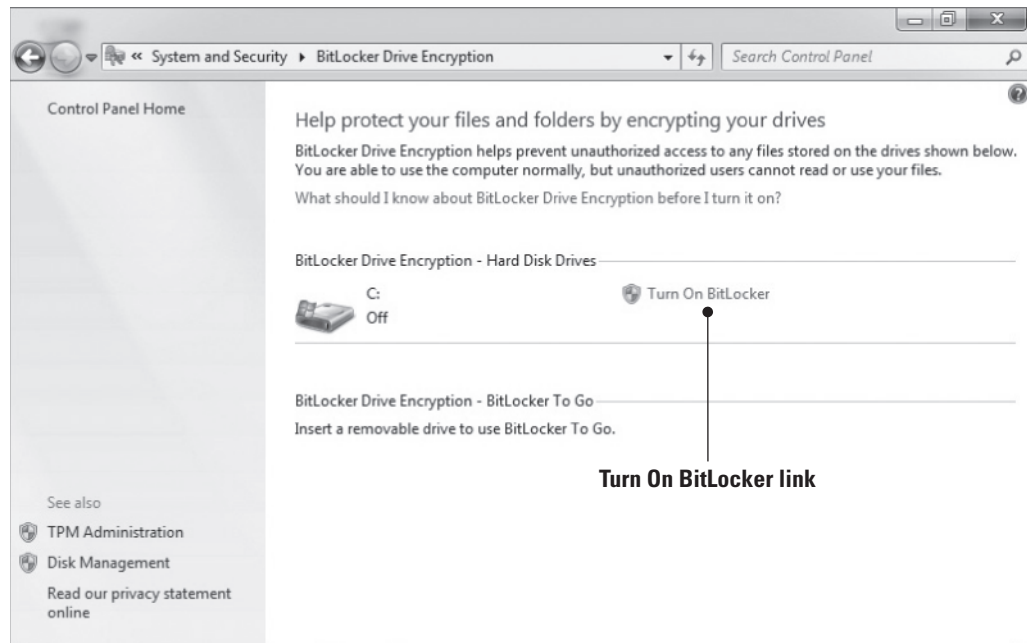
**TURN ON BITLOCKER DRIVE ENCRYPTION**

GET READY. To turn on BitLocker Drive Encryption, perform the following steps:

1. Click **Start > Control Panel > System and Security > BitLocker Drive Encryption**.
2. Click **Turn On BitLocker** for the operating system drive (see Figure 4-35). Provide an administrative password or confirm to continue, when prompted.

Figure 4-35

Turning on BitLocker



BitLocker scans your computer to ensure that it meets the BitLocker system requirements.

3. When the BitLocker Setup Wizard starts, follow the prompts to choose how to store the recovery key.
4. When prompted, confirm that the **Run BitLocker system check** check box is selected and then click **Continue** to encrypt the drive.
5. Restart the computer by clicking **Restart now**.

The encryption process might take several minutes to more than an hour. Windows displays a completion message when the encryption process is finished.

+ MORE INFORMATION

For more information about BitLocker Drive Encryption, visit <http://windows.microsoft.com/en-US/windows7/products/features/bitlocker>. For step-by-step deployment instructions, see [http://technet.microsoft.com/en-us/library/dd835565\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/dd835565(Ws.10).aspx)

SKILL SUMMARY

IN THIS LESSON YOU LEARNED:

- You install applications, or programs, either at the local level or the network level. A local installation results in the software files running directly from a computer. Installing over a network generally means the software files are made available from an application server on a network. The network method, along with Group Policy, gives an administrator more efficient control over who can use the software and who can remove it.
- Use the Programs and Features applet in Control Panel to uninstall a local application from a Windows 7 computer.
- In a Windows network in a domain environment, administrators can use Group Policy to ease the burden of administering and managing many users and client computers. Group Policy lets you control who can install software, and on which computers, and helps you push software updates and security configurations across the network.
- Services run in the background on a Windows system to help the operating system run other programs. The Services console is the central management point of services in Windows Vista and Windows 7.
- Use MSCONFIG (also known as the System Configuration utility) to troubleshoot and diagnose startup problems.
- The three primary types of file systems for Windows are FAT, FAT32, and NTFS. It's best to use NTFS-formatted disks for Windows Vista and Windows 7. NTFS handles small to very large hard disks, provides better security, and is the most reliable.
- Libraries were introduced in Windows 7. A library looks like an ordinary folder, but it is a virtual folder that simply points to files and folders in different locations on a hard disk, network drive, or external drive.
- Encrypting files and folders protects them from unwanted access. Microsoft uses the Encrypting File System (EFS) to encrypt individual files and folders in Windows Vista and Windows 7.
- Compression allows you to save disk space by reducing the size of files and folders without affecting their content.
- BitLocker Drive Encryption encrypts an entire fixed disk to prevent access by unauthorized users. BitLocker To Go protects removable drives, such as external flash drives. You can encrypt drives with BitLocker in Windows Ultimate and Enterprise editions only.

■ Knowledge Assessment

Fill in the Blank

Complete the following sentences by writing the correct word or words in the blanks provided.

1. An _____ is a program that runs “on top” of the operating system and helps a user perform a specific task, such as word processing, appointment scheduling, or accounting.
2. _____ is a collection of settings (policies) stored in Active Directory on a Windows network.
3. Windows uses _____ to handle requests for print spooling, file indexing, task scheduling, the Windows Firewall, and much more.

4. _____ allows you to enable or disable startup services, set boot options such as booting into Safe Mode, access tools like Action Center and Event Viewer, and more.
5. Most Windows Vista and Windows 7 users use the _____ file system because it supports larger disks than FAT32 or FAT.
6. Using Group Policy, you can _____ (or publish) an application to all users or computers in a designated group.
7. In Windows 7, a _____ is a virtual folder that can display content from different locations (folders, for example) on your computer or an external drive.
8. Windows uses _____ to allow users to encrypt information on hard disks, external flash disks, CDs, DVDs, backup tapes, and other types of physical media.
9. _____ is the process of decreasing the size of files or folders without affecting the files' content.
10. _____ encrypts an entire drive, rather than individual files and folders on a disk.

Multiple Choice

Circle the letter that corresponds to the best answer.

1. Which of the following can you do in the Programs and Features applet in Control Panel?
 - a. Install an application
 - b. Uninstall an application
 - c. Encrypt an application's files
 - d. Compress an application's files
2. Which of the following can you perform using Group Policy? (Choose all that apply.)
 - a. Restrict user access to an application
 - b. Encrypt a user's files
 - c. Update an application
 - d. Install applications from a network location
3. Which of the following do you access to enter Safe Mode the next time the computer starts?
 - a. The General tab
 - b. The Boot tab
 - c. The Startup tab
 - d. Services console
4. You are in the System Configuration utility and want to run Performance Monitor. Which tab do you select to start Performance Monitor?
 - a. General
 - b. Startup
 - c. Services
 - d. Tools
5. What is the maximum disk size NTFS can handle?
 - a. 32 GB
 - b. 256 GB
 - c. 32 TB
 - d. 256 TB
6. Which of the following are default libraries in Windows 7? (Choose all that apply.)
 - a. Documents
 - b. Photos
 - c. Audio
 - d. Videos

7. Which of the following settings is not configurable from the Screen Resolution window?
 - a. Orientation
 - b. Font color
 - c. Display
 - d. Windows theme
8. Where are EFS certificates stored?
 - a. EFS Certificate database
 - b. Windows Certificate database
 - c. Certificate library
 - d. Documents library
9. After you compress a folder, in what color does it display in Windows Explorer?
 - a. Blue
 - b. Green
 - c. Black
 - d. Red
10. BitLocker can use a chip, found on some computers, to protect BitLocker encryption keys. What is the name of the chip?
 - a. Trusted Platform Module
 - b. Trusted Protection Module
 - c. Encryption Platform Module
 - d. Trusted Hard Drive Module

True / False

Circle T if the statement is true or F if the statement is false.

- | | | |
|---|---|--|
| T | F | 1. Use Programs and Features to install applications in Windows 7. |
| T | F | 2. Objects in Active Directory are linked to Group Policy objects (GPOs). |
| T | F | 3. A Windows 7 system can have more than 100 services running at any one time. |
| T | F | 4. Use the Tools tab in System Configuration to enable or disable services. |
| T | F | 5. EFS and BitLocker Drive Encryption are the same thing. |

■ Competency Assessment

Scenario 4-1: Resolving Technical Problems

One of your co-workers reports that the network printer won't print. She says she has sent a print job at least 10 times but nothing prints, and she's sure the printer has paper and toner. As an IT technician, what do you do to resolve this problem?

Scenario 4-2: Protecting Laptop Computers

Henry, a traveling salesperson at your company, left his laptop at the airport on his last trip. The laptop was never recovered. His new laptop arrived yesterday and you installed Windows 7 Enterprise and productivity applications and restored data from a backup. What should you do to the laptop to protect all programs and data on the computer in the event of loss or theft?

■ Proficiency Assessment

Scenario 4-3: Uninstalling Local Software

Henry, the salesperson, left on an extended business trip to Asia. He called you one day and asked if the voice transcription software could be deleted from his computer. He doesn't use it after all and doesn't want it taking up space. What do you tell Henry to help him remove the software on his own?

Scenario 4-4: Adding Locations to a Library

Maria has two folders named AP and AR at the root of her hard disk (located at C:\). She wants to access them when she opens the Documents library. How do you advise Maria?